PCT/EP 9 9 / 0 9 0 9 0
RECD 2 8 DEC 1999
WIPO PCT

KONINKRIJK DER NEDERLANDEN

EP99/9090

Bureau voor de Industriële Eigendom

4

Hierbij wordt verklaard, dat in Nederland op 10 februari 1999 onder nummer 1011270,

ten name van:

PTT POST HOLDINGS B.V.

te Den Haag

een aanvrage om octrooi werd ingediend voor:

"Werkwijze en inrichtingen voor het afdrukken van een frankeerkenmerk op een document",

onder inroeping van een recht van voorrang, gebaseerd op de in Nederland op 20 november 1998 onder nummer 1010616 ingediende aanvrage om octrooi, en

dat de hieraan gehechte stukken overeenstemmen met de oorspronkelijk ingediende stukken.

Rijswijk, 1 oktober 1999.

De Directeur van het Bureau voor de Industriële Eigendom,
voor deze,

A.W. van der Kruk

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

10 FEB. 1999

Uittreksel

Werkwijze en stelsel voor het controleren van een frankeerkenmerk (28), dat tenminste een identificatiecode en een unieke bitstring omvat, welk stelsel middelen omvat voor:

a. inlezen van het frankeerkenmerk (28),

b. decoderen van het frankeerkenmerk (28),

c. controleren of de identificatiecode correct is door deze te vergelijken met in een geheugen (40) opgeslagen gegevens,

d. controleren of de unieke bitstring geldig is door deze te vergelijken met in het geheugen (40) opgeslagen gegevens.

[fig. 7]

2 II

10 FEB. 1999

Werkwijze en inrichtingen voor het afdrukken van een frankeerkenmerk op een document

De onderhavige uitvinding heeft betrekking op een werkwijze voor het controleren van een frankeerkenmerk, dat tenminste een identificatiecode en een unieke bitstring omvat.

Met een "frankeerkenmerk" wordt hier bijvoorbeeld verwezen naar een elektronische postzegel, dat wil zeggen een door een frankeermachine of een printer op een poststuk afgedrukt kenmerk, dat onder meer een frankeerwaarde voor het poststuk kan vertegenwoordigen. In het kader van de onderhavige uitvinding heeft "frankeerkenmerk" echter een brede betekenis. Het begrip "frankeerkenmerk" kan naar allerlei typen kenmerken verwijzen die op willekeurige documenten kunnen worden aangebracht ter beveiliging van de documenten. Dergelijke documenten kunnen behalve poststukken ook waardedocumenten zijn, zoals toegangskaarten, betaalbewijzen, enz., die met een dergelijk kenmerk worden beveiligd.

Behalve de details van het controleproces is de materie van de onderhavige uitvinding ook beschreven in Nederlandse octrooiaanvrage 1010616, waarvan de prioriteit wordt geclaimd.

Het gebruik van elektronische postzegels is bijvoorbeeld bekend uit de volgende twee door Engineering Center voor de United States Postal Service (USPS) openbaar gemaakte documenten: "Information Based Indicia Program (IBIP), Open System Indicium Specification" en "Information Based Indicia Program (IBIP), Open System Postal Security Device (PSD) Specification", beide gedateerd 23 juli 1997 (ontwerpteksten).

Met een dergelijke werkwijze kunnen elektronische postzegels worden verkregen en op poststukken worden afgedrukt. Het apparaat, bijvoorbeeld een computer, waarmee de elektronische postzegel wordt afgedrukt is daartoe voorzien van een Postal Security Device (PSD), waarbij een unieke identificatiecode behoort. De elektronische postzegel omvat diverse elementen, waarvan er enkele als "security critical" worden vermeld: de identificatiecode van de PSD, de waarde van de inhoud van een opklimmend register, de frankeerwaarde van het poststuk en een digitale handtekening. De inhoud van het opklimmende register vertegenwoordigt de totale geldwaarde van alle tot dan toe afgedrukte elektronische postzegels met de betreffende PSD. De combinatie van identificatiecode en de inhoud van het opklimmende register vertegenwoordigt een unieke

bitstring per poststuk. Aangezien de manier waarop deze unieke bitstring wordt samengesteld aan een bekende regel is gebonden, kan de waarde van een volgende unieke bitstring voor een volgende elektronische postzegel worden voorspeld, hetgeen nadelig is in verband met eventuele fraude.

In een artikel van J. Quittner in FOX Market Wire van 9 april 1998, "Neither bugs, nor hackers, nor Pitney Bows will keep E-stamp from delivering your postage", beschikbaar op Internet op 5 mei 1998, wordt een dergelijk systeem, dat aan deze specificaties voldoet en afkomstig is van de firma E-Stamp, beschreven. Het systeem van E-Stamp maakt eveneens gebruik van een personal computer voor het afdrukken van een frankeerkenmerk op een poststuk direct met behulp van een reguliere, op de personal computer aangesloten printer. De personal computer is verbonden, via het Internet, met de United States Postal Service. Via Internet kunnen aldus "elektronische postzegels" bij de United States Postal Service worden gekocht. De frankeerwaarde van de elektronische postzegel wordt direct afgeboekt van het spaartegoed van de betreffende klant en opgeslagen en beveiligd in de PSD. De PSD is een boxje dat in de achterkant van een reguliere laserprinter kan worden gestoken. Zodra een gebruiker een opdracht heeft gegeven om een elektronische postzegel op een poststuk af te drukken, wordt een elektronische postzegel gedownload en print de printer een tweedimensionale streepjescode, waarna de waarde van de afgedrukte "postzegel" van de totale frankeerwaarde in de postal security device wordt afgeboekt.

In het systeem van E-Stamp omvat de elektronische postzegel volgens de publicatie van J. Quittner in elk geval een identificatiecode van de gebruiker, een identificatiecode van de postal security device, de frankeerwaarde, het bezorgingstype (bijvoorbeeld per expres), het verzendadres en de datum. Voorts kan de elektronische postzegel ook gegevens bevatten met betrekking tot de verzendende firma en is ruimte voorzien voor eventuele advertenties.

Het doel van de onderhavige uitvinding is om een werkwijze en een stelsel te verschaffen die dergelijke elektronische postzegels kunnen controleren.

Daarom omvat de werkwijze overeenkomstig de uitvinding de volgende stappen:

a. inlezen van het frankeerkenmerk,

b. decoderen van het frankeerkenmerk,

c. controleren of de identificatiecode correct is door deze te vergelijken met in een geheugen opgeslagen gegevens,

d. controleren of de unieke bitstring geldig is door deze te vergelijken met in het geheugen opgeslagen gegevens.

Verder omvat het stelsel voor het controleren van een frankeerkenmerk, dat tenminste een identificatiecode en een unieke bitstring omvat, middelen voor:

a. inlezen van het frankeerkenmerk,

b. decoderen van het frankeerkenmerk,

c. controleren of de identificatiecode correct is door deze te vergelijken met in een geheugen opgeslagen gegevens,

d. controleren of de unieke bitstring geldig is door deze te vergelijken met in het geheugen opgeslagen gegevens.

De onderhavige uitvinding zal hierna worden toegelicht onder verwijzing naar enkele tekeningen, die slechts bedoeld zijn ter illustratie van de uitvinding en niet ter beperking daarvan. In het bijzonder heeft de uitvinding een bredere toepassing dan alleen postverkeer.

Figuur 1 toont een uitvoeringsvorm van een systeem volgens de uitvinding, waarbij gebruik wordt gemaakt van een informatiedrager waarop één of meer elektronische postzegels kunnen worden opgeslagen;

figuur 2a toont de stappen van een werkwijze voor het verstrekken van een elektronische postzegel;

figuur 2b toont de stappen van een werkwijze voor het verschaffen van de elektronische postzegel, waarbij gebruik wordt gemaakt van een teller;

figuur 3a toont de stappen voor het afdrukken van een elektronische postzegel;

figuur 3b toont de stappen voor het afdrukken van een elektronische zegel, waarbij gebruik wordt gemaakt van een teller;

figuren 4a en 4b tonen de stappen van een werkwijze volgens de uitvinding waarbij gebruik wordt gemaakt van een personal computer;

figuur 5 toont een systeem volgens de uitvinding, waarin gebruik wordt gemaakt van een personal computer;

figuur 6 toont een sorteerproces voor poststukken op schematische wijze;

figuur 7 toont enkele elementen voor het controleren van een frankeerkenmerk;

figuren 8 t/m 14 tonen stroomdiagrammen die het controleproces nader illustreren.

In figuur 1 verwijst het verwijzingscijfer 2 naar een terminal, die bijvoorbeeld in de muur van een postkantoor is aangebracht. De terminal 2 kan communiceren met een centrale 34, bijvoorbeeld via het public switched telephone network (PSTN) 46. Communicatiewegen via andere netwerken zijn uiteraard mogelijk. Daarbij kan gebruik worden gemaakt van Internet. Communicatie kan ook op andere wijze plaatsvinden, bijvoorbeeld via CDROM's, floppies, enz.

De in figuur 1 getoonde terminal 2 omvat een processor 4, die is gekoppeld met weergeefmiddelen 8 voor het communiceren met een gebruiker. Tevens omvat de terminal 2 een geheugen 6, dat met de processor 4 is verbonden. Met het verwijzingscijfer 10 is schematisch een toetsenbord aangeduid, waarmee een gebruiker gegevens en instructies voor de processor 4 kan invoeren. Daartoe is het toetsenbord 10 verbonden met de processor 4. Verder is de processor 4 verbonden met een Secure Access/Application Module 3 (meestal "SAM" genoemd).

In de in figuur 1 getoonde uitvoeringsvorm is de terminal 2 voorzien van twee invoer/uitvoereenheden 12, 14. In de invoer/uitvoereenheid 12 kan een bankpas of giropas worden ingevoerd. De invoer/uitvoereenheid 12 is daartoe voorzien van een of meer geschikte (niet getoonde) connectoren die met de bankpas en/of giropas 16 in contact kunnen worden gebracht, zoals aan de deskundige bekend is. Met een dergelijke bankpas en/of giropas kan de gebruiker zich zelf identificeren en een PIN-betaling verrichten. In het geval dat deze bankpas/giropas een elektronische beurs bevat, kan de gebruiker hiermee ook betalingshandelingen verrichten, bijvoorbeeld het betalen van een elektronische postzegel die op een poststuk moet worden afgedrukt.

De invoer/uitvoereenheid 14 is ingericht voor het opnemen van een informatiedrager 18, die een chipkaart kan zijn. Daartoe zijn de invoer/uitvoermiddelen 14 voorzien van een of meer geschikte connectoren die met de processor (niet getoond) op de chipkaart 18 contact kunnen maken, zoals aan een deskundige bekend is. Op een dergelijke informatiedrager 18 worden, in een uitvoeringsvorm van de uitvinding, een of meer elektronische postzegels opgeslagen. Dergelijke postzegels worden dan bij voorkeur beveiligd met een message authentication code (MAC) en/of beveiligd door codering opgeslagen.

In een uitvoeringsvorm is de giropas/bankpas een multifunctionele chipkaart, die onder meer voor betalingsdoeleinden kan worden gebruikt, maar ook ruimte biedt voor andere toepassingen. Een voorbeeld van een dergelijke chipkaart is de Chipper™ van de

Nederlandse KPN Telecom en Postbank. In dat geval kunnen de kaarten 16 en 18 dezelfde kaart zijn en kunnen de invoer/uitvoermiddelen 12 vervallen.

Als alternatief kan de informatiedrager 18 ook een kaart met bijvoorbeeld een magneetstrip zijn, die zelf niet is voorzien van processormiddelen. In de magneetstrip kunnen dan door de terminal 2 gegevens worden geschreven, gelezen en verwijderd. In dat geval kunnen elektronische postzegels beveiligd door codering worden opgeslagen. Het is denkbaar dat de terminal 2 een voorraad van dergelijke magneetstripkaarten heeft en dat een klant een of meer van dergelijke kaarten koopt. Op de magneetstrip kunnen dan een of meer van dergelijke elektronische postzegels zijn opgeslagen. Dergelijke magneetstripkaarten kunnen wegwerpkaarten zijn. Als wegwerpkaarten kunnen naar keuze ook chipkaarten worden gebruikt.

In figuur 1 verwijst het verwijzingscijfer 20 naar een frankeermachine. De frankeermachine 20 is voorzien van invoer/uitvoermiddelen 21 voor het opnemen van de informatiedrager 18. Tevens is de frankeermachine 20 voorzien van een processor 23, die behalve met de invoer/uitvoermiddelen 21 ook is verbonden met weegmiddelen 25, een drukeenheid 27 en een SAM 19.

Via de invoer/uitvoermiddelen 21 kan de processor 23 communiceren met de informatiedrager 18.

Met behulp van de weegmiddelen 25 kan de frankeermachine 20 het gewicht bepalen van een poststuk 22.

Met behulp van de drukeenheid 27 kan de frankeermachine 20 vervolgens informatie 29 op het poststuk 22 afdrukken.

De informatie 29 omvat bijvoorbeeld voor een mens leesbare gegevens 24 met betrekking tot de postverzendende instantie (of andere reclame), alsmede een merkteken 26 (bijvoorbeeld een streepjescode) voor het automatisch kunnen oriënteren van het poststuk in een stempel/sorteermachine, en een frankeerkenmerk 28 bijvoorbeeld in de vorm van een tweedimensionale streepjescode 28, die verdere, eventueel gecodeerde, informatie bevat. Het frankeerkenmerk 28 zal ten minste een unieke bitstring inhouden, waarvan het gebruik verderop nog zal worden toegelicht, en een identificatiecode. De identificatiecode identificeert de gebruiker, d.w.z. de persoon die de elektronische postzegel heeft aangeschaft, en/of het apparaat waarmee het frankeerkenmerk wordt afgedrukt. Indien de identificatiecode aan het afdrukapparaat is gekoppeld, kan deze bijvoorbeeld een unieke bij de SAM 19 horende code zijn. In dat geval zal de eigenaar van

de frankeermachine verantwoordelijk zijn voor eventuele fraude met het gebruik van elektronische postzegels.

Als identificatiecode van de gebruiker kan het nummer van de bankpas 16 worden gebruikt. Het bankpasnummer is immers een uniek nummer dat gekoppeld is aan de gebruiker, terwijl er een behoorlijke zekerheid kan worden verschaft, dat de gebruiker de eigenaar van de bankpas 16 is, door hem zich te laten identificeren via een PIN-code.

Voorts kan het frankeerkenmerk 28 informatie omvatten met betrekking tot de terminal 2 en de frankeermachine 20, alsmede het type postbezorging (regulier, per expres, aangetekend, per luchtpost, enz.).

Ook kan de frankeerwaarde in een voor een mens leesbare vorm 31 op het poststuk 22 zijn afgedrukt.

Op het poststuk 22 is ruimte ingeruimd voor het adres 30 van de geadresseerde.

Het in figuur 1 getoonde systeem bevat een inrichting 32 om de poststukken 22 tijdens het verzenden van de verzender naar de geadresseerde te kunnen inlezen. Indien de unieke bitstring direct een frankeerwaarde vertegenwoordigt, kan de frankeerwaarde bijvoorbeeld worden gecontroleerd. De door de inrichting 32 ingelezen gegevens worden toegevoerd aan de centrale 34. De informatie die door de inrichting 32 is ingelezen kan op elke bekende wijze aan de centrale 34 worden toegevoerd.

Voor het invoeren van de informatie naar een, in de centrale 34 aanwezige processor 36 is de centrale 34 voorzien van geschikte invoermiddelen 44, die met de processor 36 zijn verbonden.

Voor het uitvoeren van de werkwijze volgens de uitvinding is de centrale 34 bij voorkeur voorzien van drie geheugens 38, 40, 42. Dit hoeven uiteraard geen fysiek gescheiden geheugens te zijn. Zij kunnen verwijzen naar verschillende velden binnen één groter geheugen.

Figuur 2a geeft een mogelijke uitvoeringsvorm weer van de werking van de terminal 2 tijdens bedrijf.

Een klant komt bij de terminal 2 en stopt zijn bankpas 16 (hiermee zal in het vervolg zowel een bankpas/giropas of elke (multifunctionele) chipkaart worden bedoeld) in de overeenkomstige invoer/uitvoermiddelen 12. De processor 4 vraagt via de monitor 8 welk type elektronische postzegels de klant wenst te hebben. De klant kan bijvoorbeeld aangeven dat hij een frankeerpas 18 (deze benaming zal vanaf hier worden gebruikt voor

elk mogelijk type informatiedrager 18) met 100 elektronische postzegels van 80 cent wil kopen. Dit gebeurt in stap 202.

De processor 4 leest het nummer van de bankpas 16 in en vraagt de gebruiker zich te identificeren met zijn PIN-code, stappen 204 en 206.

In stap 208 controleert de processor 4 op op zichzelf bekende wijze of de klant zich correct heeft geïdentificeerd. Zo niet, dan volgt een foutmelding in stap 210. Na de foutmelding in stap 210 kan de processor 4 terugkeren naar het begin van het stroomschema dat in figuur 2a is getekend. Als alternatief kan een gebruiker, zoals op zichzelf bekend is, drie keer de mogelijkheid krijgen om de correcte PIN-code in te voeren.

Heeft een gebruiker zich op de correcte wijze geïdentificeerd, dan springt het programma in de processor 4 naar stap 212 en leest het een frankeernummer in. In overeenstemming met de uitvinding bestaat het frankeernummer uit een bitstring die uniek is en is gekozen uit een verzameling van unieke bitstrings.

De verzameling van unieke bitstrings is opgeslagen in het geheugen 38 in de centrale 34. Deze centrale 34 is met meerdere over het land verspreide terminals 2 verbonden en kan, bijvoorbeeld via het PSTN 46, één of meer unieke frankeernummers uit de verzameling unieke frankeernummers beschikbaar stellen voor de terminals 2. Daarbij kan per transactie een bepaalde hoeveelheid gewenste unieke frankeernummers uit het geheugen 38 in de centrale 34 naar het geheugen 6 in de terminal 2 worden overgedragen. Als alternatief kan ieder van de terminals 2 echter een bepaalde voorraad unieke frankeernummers vooraf in het geheugen 6 hebben opgeslagen, zodat niet iedere keer bij een transactie met een klant een verbinding tussen de terminal 2 en de centrale 34 hoeft te worden gelegd. Transmissie van de unieke bitstrings kan beveiligd op elke bekende wijze plaatsvinden.

De verzameling unieke frankeernummers in het geheugen 38 van de centrale 34 bestaat bijvoorbeeld uit bitstrings van 128 bits. Aldus bevat deze verzameling een zodanig groot aantal unieke frankeernummers, dat de behoefte aan dergelijke nummers jarenlang zal zijn gedekt.

Bij voorkeur voorafgaand aan stap 212 betaalt de klant de frankeerpas 18 op elektronische wijze. Dit gebeurt op op zichzelf bekende wijze met behulp van de bankpas 16. Dat wil zeggen dat als de bankpas 16 een reguliere bankpas is, de betaling plaatsvindt door afboeking van het banksaldo van de klant. De wijze waarop dit gebeurt is aan de

deskundige bekend en behoeft hier geen verdere toelichting. In het geval dat de bankpas 16 een elektronische beurs omvat, kan het verschuldigde bedrag direct van het saldo van de bankpas 16 worden afgeboekt. Betaling kan ook contant plaatsvinden.

De processor 4 verschaft dan via de invoer/uitvoermiddelen 14 een aparte frankeerpas 18 waarop zowel de identificatiecode als de betreffende frankeernummers zijn opgeslagen. In een uitvoeringsvorm zijn deze identificatiecode en deze frankeernummers opgeslagen met een message authentication code MAC1, die door de SAM 3 van de terminal 2 tezamen met de processor van de bankpas 16 wordt berekend. Zoals bekend is een MAC een checksum van aangeboden tekst, waarmee kan worden gecontroleerd of de aangeboden tekst valide is. Elke wijziging in de tekst (in dit geval de identificatiecode en de frankeernummers) kan worden waargenomen. Een MAC is alleen na te rekenen met een geheime sleutel, die alleen aan de SAM 3 en de bevoegde postautoriteiten bekend is. Het genereren van MAC1 en het opslaan van de nodige gegevens op de frankeerpas 18 vindt plaats in de stappen 214 en 216.

Als alternatief voor het berekenen van een MAC kunnen de gegevens ook gecodeerd worden opgeslagen.

Ter verdere beveiliging van het geheel stuurt de processor 4 bij voorkeur een kopie van de identificatiecode met de uitgegeven frankeernummers beveiligd met MAC1 en/of beveiligd door codering naar de centrale 34, die deze informatie opslaat in geheugen 40, zodat in een later stadium centraal eventuele fraude kan worden gecontroleerd, stap 218. Hierop zal hierna nog worden ingegaan.

In het geheugen van de frankeerpas 18 kan naar wens een terminalcode zijn opgeslagen, die op unieke wijze de terminal 2 identificeert, die de frankeerpas 18 heeft uitgegeven. Naar wens kan deze terminalcode onderdeel uitmaken van de berekening die MAC1 heeft opgeleverd. Dan kan namelijk ook de terminalcode niet onopgemerkt worden gewijzigd.

Figuur 3a toont een stroomdiagram van de werking van een frankeermachine 20 in overeenstemming met de werkwijze zoals toegelicht onder verwijzing naar figuur 2a.

Een gebruiker steekt zijn frankeerpas 18 in de daartoe bestemde invoer/uitvoermiddelen 21 van de frankeermachine 20. Daarmee wordt een contact tot stand gebracht tussen de frankeerpas 18 en de processor 23 van de frankeermachine 20. De gebruiker geeft via geschikte invoermiddelen (bijvoorbeeld een niet getoond toetsenbord) de processor 23 opdracht om een elektronische postzegel op poststuk 22 af te drukken. Zodra

de processor 23 heeft vastgesteld, dat een dergelijke instructie is ontvangen, stap 302, leest de processor 23 ofwel MAC1 met bijbehorende identificatiecode en frankeernummer ofwel de identificatiecode en het frankeernummer in gecodeerde vorm in van de frankeerpas 18. Indien aanwezig zal ook de terminalcode, die in de frankeerpas 18 is opgeslagen, worden ingelezen.

Op basis van de ingelezen gegevens stelt de frankeermachine 20 op vooraf bepaalde wijze een frankeerkenmerk samen en drukt dit af op het poststuk 22, stap 306. Daartoe is de frankeermachine 20 op op zichzelf bekende wijze voorzien van een opening waarin het poststuk 22 kan worden gestoken, zodat met behulp van de drukeenheid 27 het frankeerkenmerk op het poststuk 22 kan worden afgedrukt.

Het kan bijvoorbeeld zo zijn dat de processor 23 in staat is om te controleren of de frankeerwaarde genoeg is gezien het gewicht van het poststuk 22. Daartoe wordt het poststuk 22 gewogen met de weegmiddelen 25, die een weegsignaal naar de processor 23 sturen. Het frankeernummer kan bijvoorbeeld tot een bepaalde subgroep van alle unieke frankeernummers behoren, die alleen voor poststukken tot en met 50 gram mogen worden gebruikt. Per gewichtsklasse en per type postbezorging is dan een aparte subgroep unieke frankeernummers beschikbaar. Aldus kan de processor 23 direct controleren of de frankeerwaarde correct is en, indien dit niet het geval is, de gebruiker waarschuwen via een (niet weergegeven) display.

Het frankeerkenmerk wordt bijvoorbeeld in de vorm van een tweedimensionale streepjescode 28 op het poststuk 22 afgedrukt. Bij voorkeur omvat het frankeerkenmerk tenminste de volgende gegevens: het betreffende frankeernummer, de identificatiecode van de gebruiker, de terminalcode van de terminal 2, en een frankeermachinecode die de frankeermachine 20 identificeert. Bij voorkeur worden deze gegevens voorzien van een verdere MAC (MAC2) in het frankeerkenmerk afgedrukt. Een dergelijke MAC 2 wordt berekend door SAM 19 in de frankeermachine 20 tezamen met de frankeerpas 18, die daarvoor van een processor (niet getoond) moet zijn voorzien. Als alternatief kunnen de gegevens ook in gecodeerde vorm worden afgedrukt, waarbij de codering met behulp van bekende cryptografische technieken (waaronder eventueel het plaatsen van een digitale handtekening) plaatsvindt.

Naar keuze kan het frankeerkenmerk 28 ook omvatten: adresinformatie van geadresseerde en verzender (eventueel retouradres), service-informatie zoals "aangete-

kend", "per expres", enz., en datum en tijd. Deze informatie kan dan met de bovengenoemde gegevens gecodeerd worden met behulp van bekende cryptografische technieken.

Nadat de frankeermachine 20 het frankeerkenmerk op het poststuk 22 heeft afgedrukt, kan de frankeermachine 20 elk volgend gebruik van het gebruikte frankeernummer op de frankeerpas 18 onmogelijk maken. Dit gebeurt in stap 308. Dit kan bijvoorbeeld gebeuren door het betreffende frankeernummer op de frankeerpas 18 te verwijderen.

Bij verzending van het poststuk 22 van een verzender naar een ontvanger, zal het poststuk 22 op een gegeven moment in een distributiecentrum terecht komen. Daar zal het poststuk 22 met behulp van de middelen 32 worden ingelezen en kan nogmaals worden gecontroleerd of het poststuk 22 voldoende gefrankeerd is. De middelen 32 lezen ten minste het frankeerkenmerk 28 in. De middelen 32 verzamelen aldus alle ingelezen frankeerkenmerken 28 van alle poststukken, die daarvan zijn voorzien. Alle frankeerkenmerken 28 worden vervolgens verzonden naar de centrale 34 en daar door de processor 36 via de invoermiddelen 44 ingelezen. De processor 36 slaat de ingevoerde frankeerkenmerken op in het geheugen 42.

De processor 36 had in een eerder stadium reeds gegevens van de terminals 2 ontvangen met betrekking tot ofwel uitgegeven frankeernummers met bijbehorende identificatiecodes en MAC1's ofwel gecodeerde frankeernummers met bijbehorende identificatiecodes. Deze gegevens werden door de processor 36 in het geheugen 40 opgeslagen. Aldus is de processor 36 in staat om de via de invoermiddelen 44 ontvangen gegevens, na opslag in het geheugen 42, te vergelijken met de in het geheugen 40 opgeslagen gegevens. Aldus kan worden gecontroleerd of de in het geheugen 42 aanwezige frankeernummers inderdaad zijn uitgegeven. Indien er op enige wijze is geknoeid met het frankeernummer, de identificatiecode, de terminalcode en/of de frankeermachinecode, dan kan de processor 36 dit direct afleiden uit de in het frankeerkenmerk opgenomen MAC1 en MAC2 of gecodeerde gegevens. Bovendien kan de processor 36 dan herleiden bij welke terminal 2 en/of welke gebruiker onregelmatigheden hebben plaatsgevonden. De identificatiecode identificeert immers de gebruiker en/of de SAM 3 in de terminal 2 op unieke wijze.

Een verdere controle vindt plaats doordat de processor 36 bijhoudt welke unieke frankeernummers naar de terminals 2 zijn verzonden, bijvoorbeeld door deze frankeernummers op te slaan in het geheugen 40. Uiteraard kunnen deze frankeernummers ook in

een ander geheugen worden opgeslagen. Ten eerste kunnen deze reeds naar de terminals 2 verzonden frankeernummers dan niet nog een keer worden verzonden. Ten tweede kunnen de door de terminals 2 naar de centrale 34 verzonden gegevens dan reeds in een eerste ronde met de uitgegeven frankeernummers worden vergeleken, zodat direct kan worden gecontroleerd of de door de terminals 2 uitgegeven frankeernummers inderdaad frankeernummers zijn, die vanuit het geheugen 38 zijn verzonden.

Als het frankeerkenmerk 28 een identificatiecode bezit die de eigenaar van de bankpas 16 op unieke wijze identificeert, is het mogelijk om de uitvinding uit te voeren met betaling achteraf. De processor 36 kan dan immers uit de ontvangen frankeerkenmerken 28 op eenduidige wijze afleiden welke klanten welke frankeernummers hebben gebruikt. Dit opent de mogelijkheid, dat de middelen 32 bijvoorbeeld het gewicht van het poststuk 22 meten en het gewicht tezamen met het frankeerkenmerk 28 meedelen aan de processor 36. De processor 36 stelt in dat geval op dat moment vast hoeveel de klant voor het versturen van het betreffende poststuk moet betalen, een en ander afhankelijk van bijvoorbeeld het gewicht van het poststuk 22 en het type van verzending. Het betreffende bedrag wordt dan op op zichzelf bekende wijze afgeboekt van het saldo van de klant bij de bank. Uiteraard kan in plaats daarvan een factuur worden gestuurd of het saldo worden afgeboekt bij een andere bank, waarmee op op zichzelf bekende wijze een communicatieverbinding tot stand wordt gebracht. Het voordeel van deze alternatieve methode is, dat het uitgeven van frankeernummers nog niet gekoppeld is aan de waarde die nodig is gezien het gewicht en het type van verzending van het poststuk 22. Het unieke frankeernummer is dan slechts een identificatie van het poststuk 22. Het frankeernummer hoeft dan geen informatie met betrekking tot de frankeerwaarde te omvatten.

In theorie zijn er dus twee typen kaarten mogelijk: oplaadbare kaarten (bijvoorbeeld chipkaarten) en niet-oplaadbare kaarten (bijvoorbeeld magneetstripkaarten). Verder zijn in theorie in beide gevallen drie verschillende manieren van betaling mogelijk: geheel vooraf betalen van elke elektronische postzegel, geheel achteraf betalen van elke elektronische postzegel, en een combinatie van vooraf betaalde en achteraf te betalen elektronische postzegels.

Figuren 2b en 3b tonen stroomdiagrammen voor een alternatieve uitvoeringsvorm van de werkwijze volgens de uitvinding. Deze alternatieve werkwijze heeft betrekking op een uitvoeringsvorm, waarin niet per poststuk een uniek frankeernummer wordt toegepast. In sommige gevallen zou een klant bijvoorbeeld 1000 of meer poststukken willen

frankeren. Met de op dit moment beschikbare middelen voor opslag van gegevens op creditkaarten en/of van magneetstrippen voorziene kaarten is het onmogelijk om dergelijke grote aantallen unieke frankeernummers, bijvoorbeeld bestaande uit 128 bits, op te slaan. Dit probleem kan worden ondervangen door een frankeernummer met een bepaalde tellerstand te verschaffen.

De werkwijze voor het verschaffen van een elektronische zegel met teller wordt toegelicht aan de hand van figuur 2b. Stap 252 correspondeert met stap 202 uit figuur 2a.

Stap 254 geeft op verkorte wijze weer dat een gebruiker zich moet identificeren, bijvoorbeeld op de wijze zoals is toegelicht aan de hand van stappen 204-210 in figuur 2a.

Stap 256 correspondeert met stap 212 uit figuur 2a.

Nadat de processor 4 het frankeernummer heeft ingelezen, stelt de processor 4 in stap 258 een tellerstand in. Dit kan de processor 4 bijvoorbeeld doen door de gebruiker via de monitor 8 te vragen om een dergelijke tellerstand op te geven. De hoogte van de tellerstand bepaalt dan het aantal malen dat het betreffende frankeernummer mag worden gebruikt. Als alternatief kan de teller een geldwaarde vertegenwoordigen die aan elektronische postzegels mag worden besteed. De tellerstand kan de gebruiker via de toetsen van het toetsenbord 10 invoeren.

In stap 260 genereert de processor 4 MAC1 over de identificatiecode van de gebruiker, het uitgegeven frankeernummer en de tellerstand. Deze gegevens kunnen als alternatief gecodeerd worden opgeslagen. De tellerstand is dan dus ook beveiligd opgeslagen en kan niet onopgemerkt worden gewijzigd.

In stap 262 slaat de processor 4 ofwel MAC1 met de identificatiecode, het uitgegeven frankeernummer en de tellerstand ofwel de gecodeerde gegevens op op de frankeerpas 18.

De frankeerpas 18 kan weer elke uitvoeringsvorm hebben zoals hierboven is toegelicht onder verwijzing naar figuur 2a.

In stap 264 stuurt de processor 4 een kopie van MAC1 met identificatiecode, frankeernummer en tellerstand of de gecodeerde vorm van deze gegevens naar de centrale 34. De centrale 34 slaat de gegevens weer op in het geheugen 40 en dus weet deze hoe vaak het betreffende frankeernummer mag worden gebruikt.

Figuur 3b toont een stroomschema van de werking van frankeermachine 20 voor de uitvoeringsvorm waarin gebruik wordt gemaakt van een teller.

In stap 352 wacht de frankeermachine 20 totdat de klant een verzoek tot het afdrukken van een elektronische postzegel heeft gedaan. Deze stap komt overeen met stap 302 uit figuur 3a.

Zodra de klant dit verzoek heeft gedaan, leest de frankeermachine ofwel MAC1 met identificatiecode, frankeernummer en tellerstand ofwel deze gegevens in gecodeerde vorm in van de frankeerpas 18. Dit gebeurt in stap 354.

In stap 356 controleert de processor 23 of de ingelezen tellerstand nog groter dan nul is. Is dit niet het geval, dan mag het betreffende frankeernummer niet meer worden gebruikt en volgt er een foutmelding in stap 358. Het programma keert na stap 358 terug naar stap 352.

Is de tellerstand wel groter dan nul, dan gaat het programma van de processor 23 door met stap 360. In stap 360 bestuurt de processor 23 de drukeenheid 27 zodanig, dat het frankeerkenmerk, dat door de processor 23 is berekend, wordt afgedrukt op het poststuk 22. Opnieuw wordt bij voorkeur dit frankeerkenmerk voorzien van MAC2. Als alternatief worden alle gegevens gecodeerd in het frankeerkenmerk afgedrukt.

Daarna verlaagt de processor 23 in stap 362 de tellerstand op de frankeerpas 18 om aan te geven, dat het betreffende unieke frankeernummer een keer minder gebruikt mag worden, of om de beschikbare waarde te verlagen.

Uiteraard houdt de berekening van MAC2 ook rekening met de gewijzigde tellerstand.

De actuele tellerstand maakt dan onderdeel uit van het frankeerkenmerk 28 op het poststuk 22.

Opgemerkt wordt, dat de combinatie van uniek frankeernummer en actuele tellerstand dan nog steeds een unieke bitstring inhoudt. Deze laatste bitstring heeft dan alleen meer bits dan het aantal bits van het unieke frankeernummer.

De actuele tellerstand wordt dan meegelezen door de middelen 32 en vervolgens ook via de invoermiddelen 44 met behulp van de processor 36 in de centrale 34 opgeslagen in het geheugen 42. De processor 36 heeft dan de mogelijkheid om te controleren of elke combinatie van frankeernummer en tellerstand inderdaad slechts eenmaal wordt gebruikt. Aangezien de betreffende informatie beveiligd door MAC2 of beveiligd door codering is opgeslagen, is ongeoorloofde wijziging van deze getallen door de processor 36 te detecteren.

De processor 36 kan tevens controleren of de klant het frankeernummer het toegelaten aantal malen heeft gebruikt.

Het zal duidelijk zijn dat de uitvoeringsvorm volgens figuren 2b en 3b, net als de uitvoeringsvorm volgens figuren 2a en 3a, kan worden gebruikt met betaling vooraf en betaling achteraf.

Optioneel is het mogelijk om in de uitvoeringsvorm volgens figuur 1, waar gebruik wordt gemaakt van de frankeerpas 18, het gebruik van de frankeerpas 18 te beperken tot een van tevoren geselecteerd aantal frankeermachines 20. Daartoe kunnen de frankeerpassen 18 worden voorzien van die frankeermachinecodes behorend bij die frankeermachines 20, waarop gebruik van de frankeerpas 18 geoorloofd is.

Een verdere optie is om het in figuur 1 getoonde systeem zodanig uit te voeren, dat ieder van de frankeerpassen 18 ook een uniek nummer krijgt toegewezen. Dan is het mogelijk om eventuele fraude met frankeerpassen 18 te lokaliseren. Het is dan mogelijk om op een willekeurige frankeerpas 18 informatie op te laten nemen met betrekking tot die frankeerpassen 18 waarmee wordt gefraudeerd. Deze informatie met betrekking tot de frankeerpassen 18 waarmee wordt gefraudeerd, kan dan "onder water" worden overgedragen naar de frankeermachines 20, die de betreffende informatie in een (niet getoond) geheugen opslaan. Als dan een klant met een frankeerpas 18 waarmee wordt gefraudeerd een elektronische postzegel wenst af te drukken, kan de frankeermachine 20 de betreffende frankeerpas 18 detecteren en deze ongeldig maken. Dit kan gebeuren door ofwel de inhoud van de frankeerpas 18 te wissen of onleesbaar te maken, ofwel eenvoudig het afdrukken van een elektronische postzegel te weigeren. Daarmee kan verdere schade door eventuele fraude worden verminderd.

Als alternatief voor het gebruik van een teller kan ook worden gewerkt met een frankeernummer, dat bijvoorbeeld een vooraf bepaald aantal dagen door de klant mag worden gebruikt. Dit kan alleen in de uitvoeringsvorm waarmee betaling achteraf plaatsvindt. In dat geval is het frankeernummer nog steeds uniek, maar wordt het frankeernummer voor meer dan één poststuk 22 gebruikt. Omdat in dat geval een frankeerpas 18 met een bepaald uniek frankeernummer een niet vooraf bepaald aantal malen kan worden gebruikt, verdient het de voorkeur in een dergelijke uitvoeringsvorm het gebruik van een PIN-code toe te passen, die de gebruiker van de frankeerpas 18 nodig heeft om de frankeerpas 18 bij de frankeermachine 20 te kunnen gebruiken. In dat geval moet de

frankeermachine 20 zodanig zijn ingericht, dat deze de bij de frankeerpas 18 behorende PIN-code kan controleren.

Figuur 5 toont een alternatieve uitvoeringsvorm van de uitvinding, waarin gebruik wordt gemaakt van een PC van een gebruiker in plaats van een terminal 2 zoals in figuur 1 is getoond.

Onderdelen die hetzelfde zijn in figuren 1 en 5 hebben dezelfde verwijzingscijfers.

In figuur 5 verwijst verwijzingscijfer 52 naar de microprocessor van de PC 50 van een gebruiker. De microprocessor 52 is verbonden met een monitor 54, een printer 62, een toetsenbord 58 en, indien gewenst, een muis 60. In één uitvoeringsvorm is de microprocessor ook verbonden met invoer/uitvoermiddelen 14, die een bankpas 18 (multifunctionele chipcard) kunnen opnemen. Voor het berekenen van MAC's of het bepalen van coderingen van de af te drukken gegevens kan de microprocessor 52 gekoppeld zijn aan een SAM 64.

De microprocessor 52 is, bijvoorbeeld via het PSTN, verbonden met een server systeem 70, waarop meerdere computersystemen kunnen zijn aangesloten. Er kunnen meerdere server systemen zijn voorzien, ieder met hun eigen aansluitingen naar PC's. Het server systeem 70 is met de centrale 34 verbonden. Het server systeem 70 omvat een server processor 72, waarmee een SAM of HSM (= Host Security Module = een computersysteem met dezelfde functionaliteit als een SAM, maar met veel grotere capaciteit) 74 is verbonden.

Het communiceren tussen de PC 50 en het server systeem 70 kan bijvoorbeeld plaatsvinden met een internet protocol (IP).

Figuur 4a toont een stroomschema van een uitvoeringsvorm van de werking van de PC 50 in het kader van de onderhavige uitvinding voor het opladen van een bankpas 18 met een bepaald gewenst saldo, dat aan elektronische zegels kan worden besteedt. Figuur 4b betreft het daadwerkelijk afdrukken van een dergelijke elektronische zegel met een dergelijke bankpas 18.

In stap 402 wacht de microprocessor 52 totdat een gebruiker een verzoek tot het verschaffen van een saldo voor één of meer elektronische postzegels heeft gedaan. Voor het uitvoeren van een dergelijk verzoek, maakt de gebruiker gebruik van de bekende invoermiddelen, zoals toetsenbord 58 en/of muis 60. Daarbij steekt de gebruiker eerst zijn bankpas 18 in de invoer/uitvoereenheid 14.

Daarna vraagt de microprocessor 52 via de monitor 54 of de gebruiker zich op unieke wijze wil identificeren, stap 404. Dit kan bijvoorbeeld gebeuren doordat de gebruiker zijn bankpas 18 in de invoer/uitvoermiddelen 14 steekt, zodat de microprocessor 52 het nummer van de bankpas 18 kan lezen. Vervolgens zal de gebruiker zich, bijvoorbeeld met behulp van een PIN-code, moeten identificeren om duidelijk te maken dat hij de gerechtigde gebruiker van de bankpas 18 is. Controle van de PIN-code geschiedt, zoals bekend, bij voorkeur op de bankpas 18 zelf. Vervolgens kan de microprocessor 52 er van uitgaan dat de gebruiker op unieke wijze is geïdentificeerd met behulp van bijvoorbeeld het bankpasnummer. Dit gebeurt in stap 404. Als alternatief kan de microprocessor 52 de gebruiker vragen de combinatie van bankpasnummer en PIN of een andere unieke combinatie via toetsenbord 58 in te voeren, waarna deze gegevens lokaal door de PC 50 worden gecontroleerd. De PC 50 moet deze combinatie van gegevens dan wel beveiligd hebben opgeslagen.

In stap 406 vraagt de microprocessor een uniek frankeernummer op bij de centrale 34. Dit gebeurt op eenzelfde wijze als hiervoor is toegelicht onder verwijzing naar de figuren 2a en 2b.

Vervolgens genereert de SAM 74 van het server systeem 70 tezamen met de bankpas 18 een MAC, MAC1, over de identificatiecode van de gebruiker, het betreffende frankeernummer en het saldo dat voor elektronische zegels beschikbaar is gesteld. Als alternatief berekent het server systeem 70 een codering van de identificatiecode, het frankeernummer en het genoemde saldo. Dit gebeurt in stap 408.

In stap 410 slaat de microprocessor naar keuze MAC1, de identificatiecode, het frankeernummer en het genoemde saldo op op de bankpas 18. Als in plaats van een MAC-berekening een coderingsstap heeft plaatsgevonden, worden de coderingen van de identificatiecode, het frankeernummer en het genoemde saldo op de bankpas opgeslagen.

In stap 412 stuurt het serversysteem 70 een kopie van ofwel MAC1, de identificatiecode, het frankeernummer en het saldo ofwel de coderingen van de identificatiecode, het frankeernummer en het saldo naar de centrale 34. De centrale 34 zal deze gegevens weer opslaan in zijn geheugen 40.

Na stap 412 is de opslag van een saldo op de bankpas 18, dat is te gebruiken voor elektronische zegels, afgerond.

Figuur 4b toont hoe een gebruiker met zijn aldus van een saldo voorziene bankpas 18 de PC 50 kan instrueren om een frankeerkenmerk op een poststuk te printen.

Nadat het desbetreffende programma is gestart, stap 450, wacht de PC 50 totdat de gebruiker een verzoek tot het afdrukken van een frankeerkenmerk heeft gedaan, stap 452.

Via stap 454 ervaart de PC 50 hoe hoog de portokosten zijn die in het frankeerkenmerk moeten worden verwerkt. De gebruiker kan de portokosten bijvoorbeeld via het toetsenbord 58 invoeren. Het is denkbaar deze stap te automatiseren met behulp van een met de PC 50 verbonden, automatische weegschaal (niet getoond) die het poststuk weegt, waarna automatisch de portokosten worden bepaald en aan de PC 50 worden doorgegeven.

De gebruiker heeft zijn bankpas 18 weer in contact gebracht met de invoer/uitvoermiddelen 14 en zich weer geïdentificeerd met behulp van zijn PIN-code. De microprocessor 52 leest MAC1, de identificatiecode, het frankeernummer en het actuele saldo van de bankpas 18, stap 456.

De microprocessor 52 controleert vervolgens, stap 458, of het actuele saldo voldoende is voor de gewenste portokosten. Zo niet, dan volgt in stap 460 een melding aan de gebruiker, die bijvoorbeeld inhoudt dat de gebruiker zijn saldo op de bankpas moet bijladen.

In stap 462 instrueert de microprocessor 52 de printer 62 tot het afdrukken van een frankeerkenmerk, dat door de SAM 64 is berekend, op het poststuk 22 nadat de gebruiker het poststuk 22 in de printer 62 heeft ingevoerd. Daarbij berekent SAM 64 samen met de bankpas 18 MAC2 over alle gegevens die in het frankeerkenmerk zijn opgenomen, waaronder: de identificatiecode, het unieke frankeernummer, het actuele saldo en de portokosten. Als alternatief voor het berekenen van een tweede MAC, MAC2, kunnen deze gegevens gecodeerd worden. Tot de gegevens behoort bij voorkeur ook een PC-code die de PC 50 op unieke wijze identificeert.

Na stap 462 wordt in stap 464 het actuele saldo verlaagd door daarvan de portokosten af te trekken. Het nieuwe actuele saldo vertegenwoordigt dan het bedrag dat nog voor verdere elektronische zegels beschikbaar is.

Opgemerkt wordt dat bij de uitvoeringsvorm die aan de hand van figuren 4a, 4b en 5 is beschreven een uniek frankeernummer net zolang gebruikt wordt totdat het oorspronkelijke saldo is verbruikt. Omdat in elk frankeerkenmerk echter ook het actuele saldo en de actuele portokosten zijn opgenomen is er echter per poststuk nog steeds sprake van een unieke bitstring.

Na stap 464 keert het programma terug naar stap 450.

Bij voorkeur vindt de betaling door de klant direct plaats op het moment dat de klant het saldo op zijn bankpas bijlaadt. Dit kan op op zichzelf bekende wijze langs elektronische weg plaatsvinden. De afboeking kan daarbij weer plaatsvinden via de centrale 34 van een centraal banksaldo of direct van de bankpas 18 als deze een elektronische beurs omvat.

Het is echter eveneens denkbaar om betaling achteraf te laten plaatsvinden, zoals hiervoor is toegelicht onder verwijzing naar de uitvoeringsvorm van figuur 1. Daarbij vertegenwoordigt het op de bankpas 18 geladen saldo niet een totaalbedrag dat aan elektronische zegels kan worden besteed, maar het aantal malen, dat het verstrekte frankeernummer kan worden gebruikt. Het voordeel van betaling achteraf is, dat de gebruiker niet vooraf zijn poststuk 22 hoeft te wegen om de juiste frankeerwaarde in het frankeerkenmerk 28 aanwezig te laten zijn. Ook hier identificeert het frankeerkenmerk immers op unieke wijze de gebruiker, die vervolgens de rekening kan krijgen toegestuurd of van wie op automatische wijze afboeking van zijn banksaldo kan plaatsvinden. Bovendien garandeert de aanwezigheid van het unieke frankeernummer met identificatiecode, en het actuele "saldo", dat elk poststuk 22 op unieke wijze is gedentificeerd, zodat fraude direct kan worden opgemerkt.

Verder wordt opgemerkt, dat het mogelijk is om in plaats van of samen met een identificatie van de gebruiker een identificatie van de SAM 64 in het frankeerkenmerk te verwerken. In dat geval is de eigenaar van de PC 50 met SAM 64 verantwoordelijk voor de correcte betaling van de elektronische postzegels en voor eventuele met de PC 50 uitgeoefende fraude. Het is dan aan deze eigenaar om toegang tot het programma voor het aanschaffen van een elektronische postzegel aan autorisatieregels te binden.

In een verdere uitvoeringsvorm met behulp van een PC 50 kan worden gewerkt met een standaard PC zonder SAM 64. In dit geval kan de PC 50 niet op veilige wijze MAC's berekenen. Dan wordt het frankeerkenmerk ofwel centraal in de centrale 34 ofwel in server systeem 70 geproduceerd en naar de PC 50 verstuurd. De PC 50 combineert het ontvangen frankeerkenmerk dan met eventuele andere informatie en drukt deze af op het poststuk 22 met behulp van printer 62. Dan wordt dus niet meer gewerkt met opslag van een saldo voor elektronische zegels op bankpas 18, maar wordt één frankeerkenmerk per keer opgehaald bij de centrale 34. In dit geval vinden betalingen van elektronische postzegels bij voorkeur direct plaats ofwel door het afboeken van een banksaldo van de gebruiker ofwel van bankpas 18 met elektronische beurs. Om eventuele fraude te kunnen

bestrijden moet de gebruiker zich dan op unieke wijze identificeren, bijvoorbeeld met zijn giro/banknummer en een bijbehorende PIN. Identificatie vindt dan bij voorkeur nog steeds plaats met bankpas 18 en het controleren van een PIN-code.

In het voorgaande is beschreven hoe een frankeerkenmerk met een unieke bitstring kan worden gegenereerd en op een document kan worden afgedrukt. Claims gericht op dit proces zijn op 20 november 1998 ingediend met de Nederlandse octrooiaanvrage 1010616, waarvan de prioriteit is geclaimd. Hieronder zal nader worden ingegaan op de verwerking van documenten voorzien van een dergelijk frankeerkenmerk, en met name op de controle van de geldigheid daarvan. Daarbij zal als voorbeeld worden ingegaan op de situatie, dat de documenten poststukken betreffen. Zoals eerder gesteld hoeven de documenten echter geen poststukken te zijn.

Eerst zal een korte beschrijving worden gegeven van het "BriefPost 2000" systeem, dat door de Nederlandse PTT Post is ontwikkeld. Daarna wordt beschreven, hoe het frankeerkenmerk kan worden gecontroleerd in het sorteerproces.

BriefPost 2000.

Automatisch sorteren binnen BriefPost 2000 is schematisch uiteen gezet in figuur 6 en valt uiteen in twee produktieprocessen, voor het sorteren van respectievelijk "Briefpost Klein", respectievelijk Briefpost Groot, dat betrekking heeft op kleine, respectievelijk grote poststukken.

Deze twee categorieën worden door verschillende machines gesorteerd. Echter, beide categorieën omvatten in principe dezelfde, maar gescheiden uitgevoerde sorteergangen:

1. eerste sorteergang: deze sorteert de post voor de sorteercentra;

2. tweede sorteergang: deze sorteert de post voor het bestellen op het postadres of voor het afleveren in een postbus.

In de eerste sorteergang wordt, uitgaande van de informatie van het adresbeeld van de post, door het codeercomputernetwerk de sorteerinformatie bepaald. Het systeem heeft daarvoor in principe 30 sec. de tijd - gedurende die tijd is het poststuk fysiek in de sorteermachine aanwezig (geldt niet bij de sorteermachine voor Briefpost Groot). De sorteerinformatie wordt vervolgens op de post aangebracht in de vorm van indexen:

1. sorteerindex (SIX): deze index wordt voor Briefpost Klein aangebracht bij succesvolle "codering"; in de eerste sorteergang wordt hiermee de sorteerinformatie vastgelegd, bijvoorbeeld als barcode op de post. In de tweede sorteergang kan deze vervolgens betrouwbaar worden gelezen;

2. identificatieindex (IX): deze wordt voor Briefpost Groot aangebracht, of indien bij Briefpost Klein de codering niet tijdig beschikbaar is. Er wordt geen sorteerindex (SIX) afgedrukt, maar een volgnummer (IX) geplaatst. Eventuele sorteerinformatie wordt dan gerelateerd aan dit nummer in het computernetwerk opgeslagen. Bij de sorteermachine voor Briefpost Groot gebeurt dit voor alle poststukken i.v.m. een te korte mechanische vertragingslijn, bij de sorteermachine voor Briefpost Klein wordt deze methode alleen gehanteerd indien de sorteerinformatie niet tijdig (binnen 30 sec.) beschikbaar is. In de tweede sorteergang wordt de sorteerinformatie aan de hand van de identificatieindex opgezocht. Bij Briefpost Klein kan ook een identificatieindex gebruikt worden als de codeercomputer de sorteerinformatie niet binnen een bepaalde tijd kan achterhalen. De post moet dan later opnieuw de eerste sorteergang doorlopen;

3. klantindex (KIX): deze index bevat bijvoorbeeld de postcode en het huisnummer, postbusnummer of antwoordnummer, bijvoorbeeld in de vorm van een barcode. Dit is een index die door klanten als onderdeel van het adres op de post kan worden vastgelegd;

4. speciale klantindex: dit is een interne door de Nederlandse PTT Post gebruikte index die via stickers op poststukken wordt aangebracht. Deze index wordt bijvoorbeeld gebruikt bij verhuispost-service.

Het codeerproces maakt, voor de eerste sorteergang Briefpost Klein, onderscheid tussen on-line en off-line codering:

1. on-line codering: dit is het proces waarbij binnen een bepaalde tijd (30 sec.) de sorteerinformatie van de post wordt vastgesteld;

2. off-line codering: dit is het proces waarbij, als de on-line codering niet gelukt is vanwege een tijdsoverschrijding, de post voorzien wordt van een identificatieindex (IX) en vervolgens uit de geassocieerde opgeslagen adresbeelden alsnog de sorteerinformatie wordt vastgesteld, welke na een tweede doorloop van de eerste sorteergang alsnog op de post wordt aangebracht.

Figuur 7 toont een voorbeeld van een codeernetwerk, dat bij de onderhavige uitvinding kan worden gebruikt. Het codeernetwerk bestaat uit een codeercomputer CC en diverse codeermiddelen:

1. codeercomputer CC (Coding Computer): deze verdeelt het codeerwerk over de codeermiddelen en bepaalt per poststuk de te voeren codeerstrategie;

2. eerste adreslezer PCD (Primary Coding Device): deze bepaalt de sorteerinformatie voor de bulk van alle post;

3. tweede adreslezer SCD (Secondary Coding Device): deze tracht de sorteerinformatie te bepalen voor post die niet door de eerste adreslezer is gecodeerd;

4. adreszoeksysteem ADB (Adres Database): dit tracht in het geval van onbetrouwbare resultaten van de eerste adreslezer PCD en of tweede adreslezer SCD alsnog betrouwbare sorteerinformatie te bepalen;

5. videocodeerstation VCD (Video Coding Device): hier kan de sorteerinformatie handmatig voor de overgebleven post worden bepaald;

6. decodeereenheid DD (Decoding Device) die is ingericht voor het decoderen van frankeerkenmerken 28 van uitgelezen poststukken.

Opgemerkt wordt dat verdere of alternatieve codeermiddelen in de toekomst mogelijk zijn.

Het codeernetwerk is verbonden met de sorteermachines. Een belangrijk onderdeel van de sorteermachine zijn een of meer Mail Transport Units MTU. Elke MTU is ingericht om indexen te lezen en printen. Tevens is elke MTU voorzien van een camera 100 om beelden van de post op te nemen die als input dienen voor de codeercomputer.

Voordat de post door een van de MTU's wordt verwerkt is deze geschift (d.w.z. ingedeeld in Briefpost Klein en Briefpost Groot), opgezet in bakken (d.w.z. elk poststuk heeft een uniforme positie van adreszijde en frankeeraanduiding; hiervoor wordt bij voorkeur gebruik gemaakt van merkteken 26 op het poststuk) en gestempeld (d.w.z. ontwaarden van postzegels of gedrukte frankeerwaarde). Dit gebeurt bij voorkeur met behulp van een Schift-, Opzet-, en Stempelmachine SOSMA. De SOSMA heeft de taak om bepaalde bulkstromen te scheiden van de rest (bijvoorbeeld giro-opdrachtenveloppen etc.). Hiervoor wordt de FIM-code toegepast.

Barcodelezer.

Er zijn verschillende opties voor de wijze waarop de barcode 28 in het proces gelezen kan worden.

Er kan bijvoorbeeld gebruik gemaakt worden van de beelden die met de camera's 100 in de sorteermachines worden gemaakt als input voor het codeerproces; uit deze beelden kan via een speciale, met de camera's 100 verbonden codeereenheid de inhoud van de barcodes worden terug bepaald. Dit veroorzaakt echter een forse toename van de gegevensstromen in het codeernetwerk, omdat 100 % van alle beelden extra naar een dergelijke codeereenheid moet worden gezonden.

Een andere mogelijkheid is toepassing van een dedicated barcodelezer die als uitgangsdata bijvoorbeeld een "ascii-string" oplevert, welke vervolgens via het codeernetwerk verder getransporteerd kan worden naar een verificatiedatabasesysteem. Een dergelijke barcodelezer kan naar keuze bijvoorbeeld in de sorteermachine, maar ook in de SOSMA worden ingebouwd. In dit geval wordt de impact op het sorteerproces minimaal, en ook van nagenoeg alle met de hand te verwerken poststromen kunnen hiermee de barcodes 28 worden gecontroleerd.

Soms zal het bezorgadres, of tenminste de postcode daarvan, zijn opgenomen in het frankeerkenmerk. Op het moment van lezen van het frankeerkenmerk komt dus ook tenminste een essentieel deel van het bezorgadres beschikbaar. Deze informatie kan ten eerste worden gebruikt om het uitlezen van het afgedrukte bezorgadres 30 met een Optical Character Recognition (OCR) eenheid te bespoedigen en ten tweede om direct vast te stellen of er onregelmatigheden met het bezorgadres (en dus wellicht met het gebruik van de unieke bitstring) hebben plaatsgevonden.

Unieke bitstrings & frankeerkenmerk.

Zoals eerder beschreven kan de aanwezigheid van een unieke bitstring in het frankeerkenmerk 28 worden gebruikt als middel om de geldigheid van een frankering (of van een willekeuring document) aan te geven. Uitgangspunt bij de methode is het gebruik van een nieuwe unieke bitstring voor elke transactie. Dus een unieke bitstring is in dat geval slechts 1 maal geldig. Zoals vermeld kunnen beperkingen in de opslagcapaciteit van o.a. smart cards ertoe leiden, dat dit uitgangspunt bij de huidige (betaalbare) stand der techniek niet haalbaar is (een smart card waarmee slechts enkele, bijvoorbeeld minder dan 10, transacties mogelijk zijn, heeft nauwelijks praktisch nut). Een oplossing hiervoor is gevonden in toepassing van een "purse" of counter op de

smart card in combinatie met een unieke bitstring. Een dergelijke unieke bitstring is dan meerdere malen geldig, bijvoorbeeld in combinatie met een vooraf nauwkeurig gedefinieerd saldo.

Controles.

De controles beperken zich tot die welke in het sorteerproces mogelijk zijn. Figuren 8 t/m 14 tonen stroomschema's ter verduidelijking van de controles.

Scannen van het frankeerkenmerk (figuur 8).

Het poststuk 22 (brief) wordt door de MTU met de camera 100 ingelezen ten behoeve van het vaststellen van de adresgegevens, stap 800. Hierbij wordt een volledig beeld van de voorkant van het poststuk gemaakt.

In dit beeld wordt de (twee dimensionale) barcode 28 gezocht, stap 802. Vervolgens wordt geanalyseerd of de barcode 28 een elektronisch zegel in de zin van de uitvinding bevat, stap 804. Is dit niet het geval, dan wordt het poststuk als reguliere post verwerkt, stap 806.

Is een elektronische zegel aanwezig, dan wordt de barcode 28 geïnterpreteerd/gedecodeerd, zodat de informatie beschikbaar komt, stap 808 (zie volgende sectie). Hiervoor zou in het codeernetwerk (figuur 6) naast de PCD en de SCD een speciale decodeereenheid DD (Decoding Device) geïntegreerd kunnen worden.

Kan om een of andere reden het frankeerkenmerk niet correct worden gedecodeerd, stap 810, dan wordt het poststuk naar een aparte verwerking geleid, stap 812. Vervolgens wordt het Proof-of-Payment veld gevalideerd, stap 814.

Decoderen van frankeerkenmerk (stap 808).

Het frankeerkenmerk 28 bevat bijvoorbeeld een 2D DataMatrix barcode. Deze bevat verschillende informatie-eenheden waaronder een digitale handtekening van de afzender (frankeerder), versleutelde (geëncrypte) informatie, en niet-versleutelde gegevens (elementen). De versleutelde informatie is zelf weer opgebouwd uit gegevenselementen. Voor de digitale handtekening en de versleuteling wordt public key cryptography gebruikt, waarbij de digitale handtekening met behulp van de private

key van de afzender wordt gegenereerd, en de versleuteling plaatsvindt met de (van toepassing zijnde) public key van PTT Post.

Een eerste controle vindt plaats op basis van de digitale handtekening. Ten behoeve van de controle op de betaling wordt het proof-of-payment gevalideerd (stap 814).

Valideren Proof-of-Payment (stap 814).

Het Proof-of-Payment bevat een aantal data- en controle-elementen. De controle-elementen zijn (bijvoorbeeld) MACs die de data-elementen beschermen (bescherming kan ook via codering of versleuteling plaatsvinden). De data-elementen zijn het frankeerkenmerk en de identificaties van het betaalmiddel (bijvoorbeeld smart card 16/18), de uitgiftemachine 2, 50 en de frankeermachine 20 (of printer 62, indien gewenst), en de betaling. Zie figuur 9, waarin de volgende stappen van het valideringsproces bij gebruik van MACs zijn getoond (bij gebruik van codering of versleuteling is het schema analoog):

1. lees MAC's in, stap 902, en controleer of de ingelezen MACs valide zijn, stap 904. Indien dit niet het geval is, dan is de frankering niet valide en wordt een apart proces, stap 906, uitgevoerd.

2. Indien de MACs valide zijn, lees de identificaties van de uitgiftemachine 2, 50 en frankeermachine 22 (printer 62) bestaan, stap 908 en controleer hun geldigheid, stappen 908 - 912.

3. Lees de identificatie van het betaalmiddel en controleer of deze een plausibele is. Dit kan ook in de stappen 908 -912 worden uitgevoerd en is geen harde controle.

4. Tenslotte moet de geldigheid van de betaling geverifieerd worden door te controleren of er een geldig (nieuw, maar uitgegeven) frankeerkenmerk is afgedrukt op het poststuk 22, stap 914. Dit betreft een eenvoudige look-up in de tokendatabase in het tweede geheugen 40 plus het markeren van afgedrukt zijn van de betreffende unieke bitstring. Indien de methode van "unieke bitstring plus teller", waarbij de teller ofwel een aantal malen dat de bitstring mag worden gebruikt ofwel een saldo definieert, wordt toegepast, geldt het volgende: de combinatie van unieke bitstring en teller moet worden gecontroleerd. Zoals eerder opgemerkt, is de combinatie van bitstring, hoewel vaker gebruikt dan één keer, en teller nog steeds uniek voor

iedere frankering. Als eerste kan met behulp van de database 40 de geldigheid van de unieke bitstring worden bepaald. Immers, deze moet uitgegeven zijn. Als de bitstring een bepaalde geldigheidsduur heeft gekregen, kan ook deze worden gecontroleerd. Afhankelijk van de betalingswijze (voor verstrekken van de unieke bitstring of na verwerking van een betreffend poststuk door de posterij) zal bijgehouden moeten worden wat verstrekt en\of afgedrukt is. In het geval van niet verstrekte, reeds eerder afgedrukte, en/of niet langer geldige unieke bitstrings is de frankering niet valide.

Als er sprake is van een unieke bitstring, waarbij een bepaald saldo hoort, zal in geheugen 40 de combinatie van die bitstring en dat saldo (tellerstand) aanwezig moeten zijn. Concreet moet blijken dat een dergelijke combinatie nog niet eerder op een poststuk werd afgedrukt. Vervolgens moet deze combinatie als zijnde afgedrukt en niet meer geldig worden aangemerkt.

In de database 40 kunnen bij iedere unieke bitstring de volgende gegevens zijn vastgelegd:

1. de uitgiftedatum en geldigheidsduur,

2. de toegestane betalingswijze (voor het verstrekken daarvan of na afdrukken op een poststuk) en

3. op poststukken afgedrukte combinaties van de bitstring met saldo (tellerstanden). N.B. het is ook mogelijk om alleen een actuele tellerstand centraal bij te houden en steeds bij waarnemen van een bitstring met een bepaalde tellerstand, deze centraal geregistreerde tellerstand aan te passen. Dit zal hierna nog worden toegelicht.

Verwerking en controle op basis hiervan is uitgelegd aan de hand van stappen 1002 - 1014 in het stroomschema van figuur 10, dat voor zich zelf spreekt.

Afhankelijk van de betalingswijze, vooraf of achteraf betaald, wordt het verbruik anders geregistreerd. Tevens zijn er simpelere en meer fundamentele implementaties van de controles mogelijk, zoals hierna zal worden toegelicht.

Betaling vooraf ("pre-paid").

Bij pre-paid kaarten 18 is er in principe een bepaalde set unieke bitstrings op de kaart aanwezig, die bij verkoop van de kaart 18 als zodanig in de database 40 worden gemerkt. De unieke bitstrings kunnen elk een bepaalde (vaste) waarde vertegenwoordigen of elk in combinatie met een teller (saldo) worden verbruikt. In ieder geval geldt: na verbruik van de teller(s) zijn de unieke bitstrings ongeldig.

Voor de pre-paid bitstrings wordt het initiële saldo geregistreerd (per unieke bitstring of totaal per kaart 18, d.w.z. per set unieke bitstrings). Voor iedere frankering wordt dan een gedeelte van dit saldo afgehaald. Als het saldo opgebruikt is, dan is de bitstring opgebruikt.

Het controle-proces is gelijk aan dat van de "normale" oplaadbare kaarten.

In eerste instantie kan de simpele methode, figuur 11, geïmplementeerd worden, totdat er voldoende aanleiding is om de meer fundamentele, figuur 12, te implementeren.

Simpel.

In het meest simpele geval, zoals toegelicht aan de hand van stappen 1102 - 1108 in figuur 11, wordt alleen een totaalstand bijgehouden. Hierdoor is het niet mogelijk om bijvoorbeeld kopieën te detecteren voordat de centraal (geheugen 40) geregistreerde tellerstand nul is geworden. Er is wel de garantie dat uiteindelijk het misbruik ontdekt zal worden en dat het totale misbruik niet meer kan zijn dan het initiële saldo.

Fundamenteel.

Als alle frankeringen worden geregistreerd, d.w.z. dat bij de unieke bitstrings is geregistreerd welke tellerstanden daadwerkelijk op een poststuk zijn afgedrukt, dan zijn kopieën te detecteren. De individuele tellerstanden moeten reflecteren dat de initiële tellerstand aaneensluitend is verbruikt. Dit is verder uitgelegd aan de hand van stappen 1202 - 1208 in het stroomschema van figuur 12.

De initiële tellerstand is te beschouwen als een interval. Iedere tellerstand is daaruit een subinterval. Nu moet de doorsnijding van elk tweetal subintervallen leeg zijn, en moet de vereniging van alle subintervallen de intitiële tellerstand overdekken. Dit laatste hoeft niet in zijn geheel te gebeuren, bijvoorbeeld omdat bepaalde gefrankeerde poststukken nooit voor bezorging aangeboden zijn, of omdat een gedeelte van het saldo nog niet gebruikt is.

Betaling achteraf ("post-paid").

Ook hier gelden twee methodes. Principieel wordt voor elke transactie een unieke bitstring "verbruikt".

Om implementatie-technische redenen kan gekozen worden voor het verbruik van een unieke bitstring voor een te definiëren reeks van transacties. Naast "verbruik" van de bitstring wordt hier bij het frankeren een teller toegepast die net als in conventionele frankeermachines het in rekening te brengen verbruik registreert.

Aan het te verbruiken saldo kan een limiet gesteld worden (in tijd of in geld). Bij overschrijding is heropladen van de kaart 18 vereist.

Bij post-paid wordt bijvoorbeeld voor iedere frankering een teller met één of de gefrankeerde waarde opgehoogd. Dit kan tot een bepaalde limiet is bereikt, waarna het eerder genoemde heropladen van de kaart vereist is. Op het moment van heropladen kan de kaarthouder "kwijting" krijgen voor het gebruik tot op dat moment mits uiteraard ingestaan wordt voor betaling van het gefrankeerde.

Een implementatievariant bestaat uit het feitelijk verlagen van de teller vanaf een maximumwaarde, welke eenvoudig bij aanschaf ingesteld kan worden. Zodra de teller op 0 is aangekomen, is de bitstring ongeldig geworden. Voor ongelimiteerd gebruik kan de limiet dan op een zeer grote waarde worden gezet, die in de praktijk groot genoeg is.

Simpel.

Als wordt afgezien van de controle op duplicaten, dan kan in eerste instantie worden volstaan met het bijhouden van het aantal frankeringen: zie stappen 1302 - 1308 in figuur 13. De optie van verbruikssaldo is in de figuur niet aangegeven, maar werkt analoog.

Fundamenteel.

Voor controle op duplicaten zullen alle individuele tellerstanden bij de unieke bitstring moeten worden bijgehouden. In principe is bijvoorbeeld een bitmap hiertoe een geëigend middel. Dit is verder uitgelegd aan de hand van stappen 1402 - 1408 in figuur 14. Doordat de tellerstanden in principe opeenvolgend zijn, en eenmaal gefrankeerde poststukken binnen een gelimiteerde periode moeten worden aangeboden, kan de actuele grootte van de bitmap beperkt worden door bij te houden welke tellerstand de laatste voor de ingang van de betreffende periode was. Deze stand en de bitmap worden dagelijks aangepast. Ook hier is de optie van het gebruik van een verbruikssaldo niet in de figuur opgenomen.

nodig zal zijn. Een dergelijke voordelige volgorde kan bijvoorbeeld (alfa)numeriek zijn.

De controle kan fysiek plaatsvinden in de centrale 34. In plaats daarvan kan de controle echter ook op een aantal geografisch gescheiden locaties plaatsvinden, bijvoorbeeld op die locaties waar de tweede sorteergang plaatsvindt. Hierdoor is het onderhouden van één centrale database in centrale 34 lastiger, want dit vereist transport van uitgegeven unieke bitstrings naar de gescheiden controlecentra via een gegevensdrager of via een adequate netwerkverbinding tussen de controlecentra en de centrale 34. Merk op dat (illegale) duplicaten van frankeerkenmerken op bij verschillende sorteercentra aangeboden poststukken in de tweede sorteergang te identificeren zijn.

In het geval het bezorgadres beveiligd in het frankeerkenmerk is opgenomen, is het niet meer mogelijk om op eenvoudige wijze het frankeerkenmerk te kopiëren om post naar verschillende bezorgadressen (ontvangers) te sturen.

Conclusies

1. Werkwijze voor het controleren van een frankeerkenmerk (28), dat tenminste een identificatiecode en een unieke bitstring omvat, omvattende de volgende stappen:
   a. inlezen (800-804) van het frankeerkenmerk (28),
   b. decoderen (808-810) van het frankeerkenmerk (28),
   c. controleren (908-910) of de identificatiecode correct is door deze te vergelijken met in een geheugen (40) opgeslagen gegevens,
   d. controleren (1002-1014) of de unieke bitstring geldig is door deze te vergelijken met in het geheugen (40) opgeslagen gegevens.
2. Werkwijze volgens conclusie 1, waarbij de identificatiecode en de unieke bitstring beveiligd zijn met behulp van een Message Authentication Code en/of door middel van codering en de werkwijze ook de stap omvat van het controleren (902-904) van de Message Authentication Code en/of de codering.
3. Werkwijze volgens conclusie 1 of 2, waarbij het frankeerkenmerk een terminalidentificatiecode omvat die bij een terminal behoort die de unieke bitstring aan een gebruiker heeft verstrekt.
4. Werkwijze volgens een van de voorgaande conclusies, waarbij de identificatiecode een gebruikersidentificatiecode en/of een afdrukidentificatiecode omvat, welke afdrukidentificatiecode behoort bij een afdrukeenheid die het frankeerkenmerk heeft afgedrukt.
5. Werkwijze volgens een van de voorgaande conclusies, waarbij het frankeerkenmerk een combinatie van de unieke bitstring en een tellerwaarde omvat en de werkwijze tevens de volgende stappen omvat:
   e. aftrekken van de tellerwaarde van een bij die unieke bitstring opgeslagen resterende tellerstand in het geheugen (40) en controleren of de resterende tellerstand meer bedraagt dan nul, en zo ja, dan vaststellen dat het frankeerkenmerk geldig is en zo niet, dan vaststellen dat het frankeerkenmerk ongeldig is.
6. Werkwijze volgens een van de conclusies 1 t/m 4, waarbij het frankeerkenmerk een combinatie van de unieke bitstring en een tellerwaarde omvat en de werkwijze tevens de volgende stappen omvat:

f. controleren of deze combinatie voorkomt in het geheugen (40), zo ja, dan vaststellen dat het frankeerkenmerk geldig is, zo niet, dan vaststellen dat het frankeerkenmerk ongeldig is.

7. Werkwijze volgens een van de voorgaande conclusies, waarbij tevens wordt gecontroleerd of een bij het frankeerkenmerk horende geldigheidstermijn is verlopen.

8. Werkwijze volgens conclusie 5, 6 of 7, waarbij, indien is vastgesteld dat het frankeerkenmerk geldig is, een routine wordt gestart voor het automatisch achteraf betalen van een bij het frankeerkenmerk horende rekening.

9. Werkwijze volgens een van de voorgaande conclusies, waarbij het frankeerkenmerk zich op een poststuk bevindt dat ten behoeve van bezorging in ten minste een eerste en daarna een tweede sorteercentrum wordt gesorteerd, dat de stappen a en b worden uitgevoerd in het eerste sorteercentrum en de daaruit verkregen informatie naar een controlecentrum wordt gestuurd, waarna de stappen c en d worden uitgevoerd in het controlecentrum voorafgaand aan sortering in het tweede sorteercentrum.

10. Stelsel voor het controleren van een frankeerkenmerk (28), dat tenminste een identificatiecode en een unieke bitstring omvat, omvattend middelen voor:

a. inlezen van het frankeerkenmerk (28),

b. decoderen van het frankeerkenmerk (28),

c. controleren of de identificatiecode correct is door deze te vergelijken met in een geheugen (40) opgeslagen gegevens,

d. controleren of de unieke bitstring geldig is door deze te vergelijken met in het geheugen (40) opgeslagen gegevens.

11. Stelsel volgens conclusie 10, waarbij de identificatiecode en de unieke bitstring beveiligd zijn met behulp van een Message Authentication Code en/of door middel van codering en het stelsel ook middelen omvat voor het controleren (902-904) van de Message Authentication Code en/of de codering.

12. Stelsel volgens conclusie 10 of 11, waarbij het frankeerkenmerk een terminalidentificatiecode omvat die bij een terminal behoort die de unieke bitstring aan een gebruiker heeft verstrekt.

13. Stelsel volgens een van de conclusies 10 t/m 12, waarbij de identificatiecode een gebruikersidentificatiecode en/of een afdrukidentificatiecode omvat, welke

afdrukidentificatiecode behoort bij een afdrukeenheid die het frankeerkenmerk heeft afgedrukt.

14. Stelsel volgens een van de conclusies 10 t/m 13, waarbij het frankeerkenmerk een combinatie van de unieke bitstring en een tellerwaarde omvat en het stelsel tevens middelen omvat voor:

e. aftrekken van de tellerwaarde van een bij die unieke bitstring opgeslagen resterende tellerstand in het geheugen (40) en controleren of de resterende tellerstand meer bedraagt dan nul, en zo ja, dan vaststellen dat het frankeerkenmerk geldig is en zo niet, dan vaststellen dat het frankeerkenmerk ongeldig is.

15. Stelsel volgens een van de conclusies 10 t/m 14, waarbij het frankeerkenmerk een combinatie van de unieke bitstring en een tellerwaarde omvat en het stelsel tevens middelen omvat voor:

f. controleren of deze combinatie voorkomt in het geheugen (40), zo ja, dan vaststellen dat het frankeerkenmerk geldig is, zo niet, dan vaststellen dat het frankeerkenmerk ongeldig is.

16. Stelsel volgens een van de conclusies 10 t/m 15, tevens voorzien van middelen om te controleren of een bij het frankeerkenmerk horende geldigheidstermijn is verlopen.

17. Stelsel volgens conclusie 14, 15, of 16, dat, indien is vastgesteld dat het frankeerkenmerk geldig is, een routine start voor het automatisch achteraf betalen van een bij het frankeerkenmerk horende rekening.

18. Stelsel volgens een van de conclusies 10 t/m 17, waarbij het frankeerkenmerk zich op een poststuk bevindt dat ten behoeve van bezorging in ten minste een eerste en daarna een tweede sorteercentrum wordt gesorteerd, en het stelsel in het eerste sorteercentrum opgestelde middelen omvat voor het uitvoeren van de stappen a en b en voor het verzenden van de uit stappen a en b verkregen informatie naar een controlecentrum, en het controlecentrum middelen omvat voor het uitvoeren van de stappen c en d voorafgaand aan sortering in het tweede sorteercentrum.

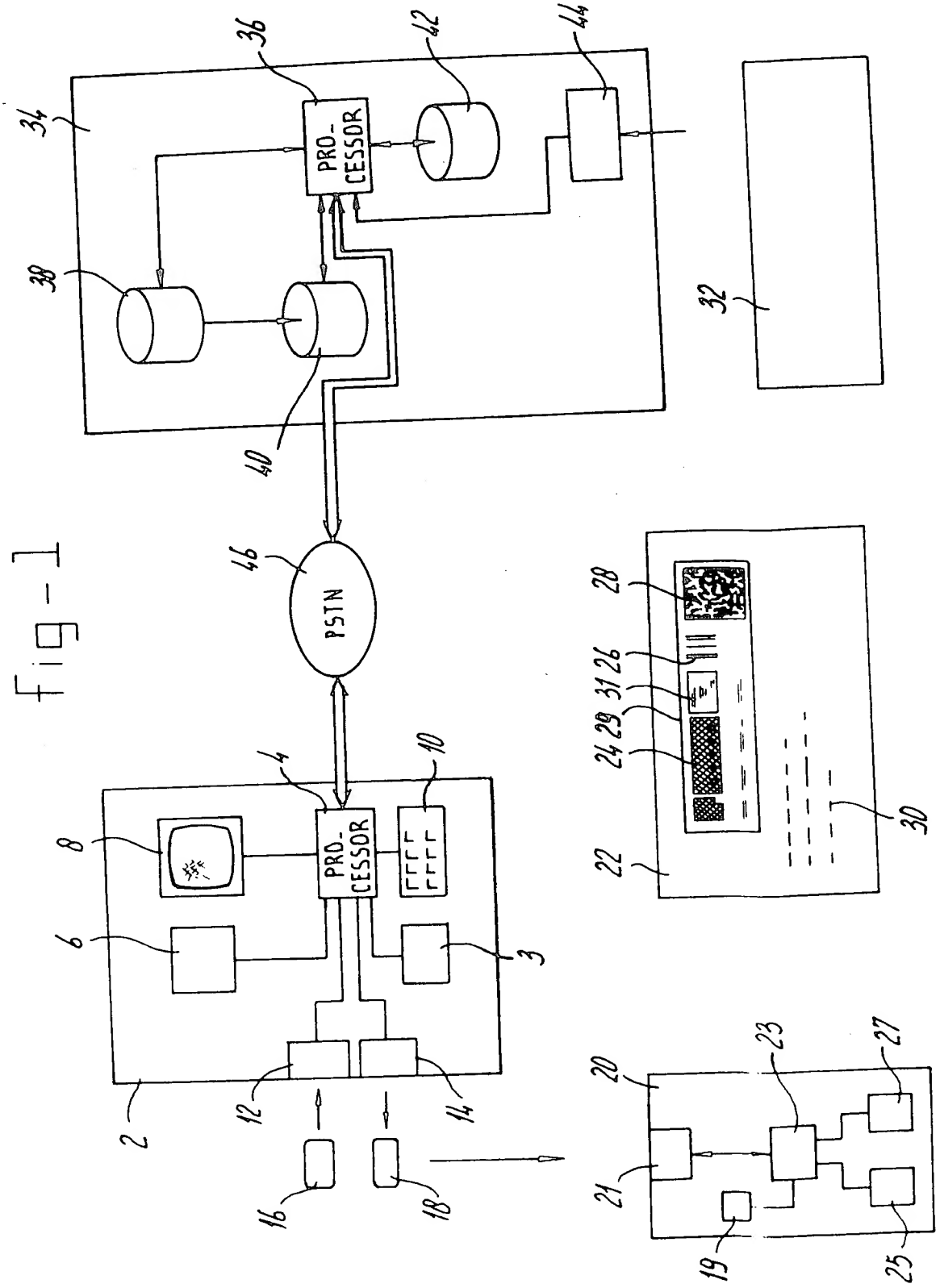
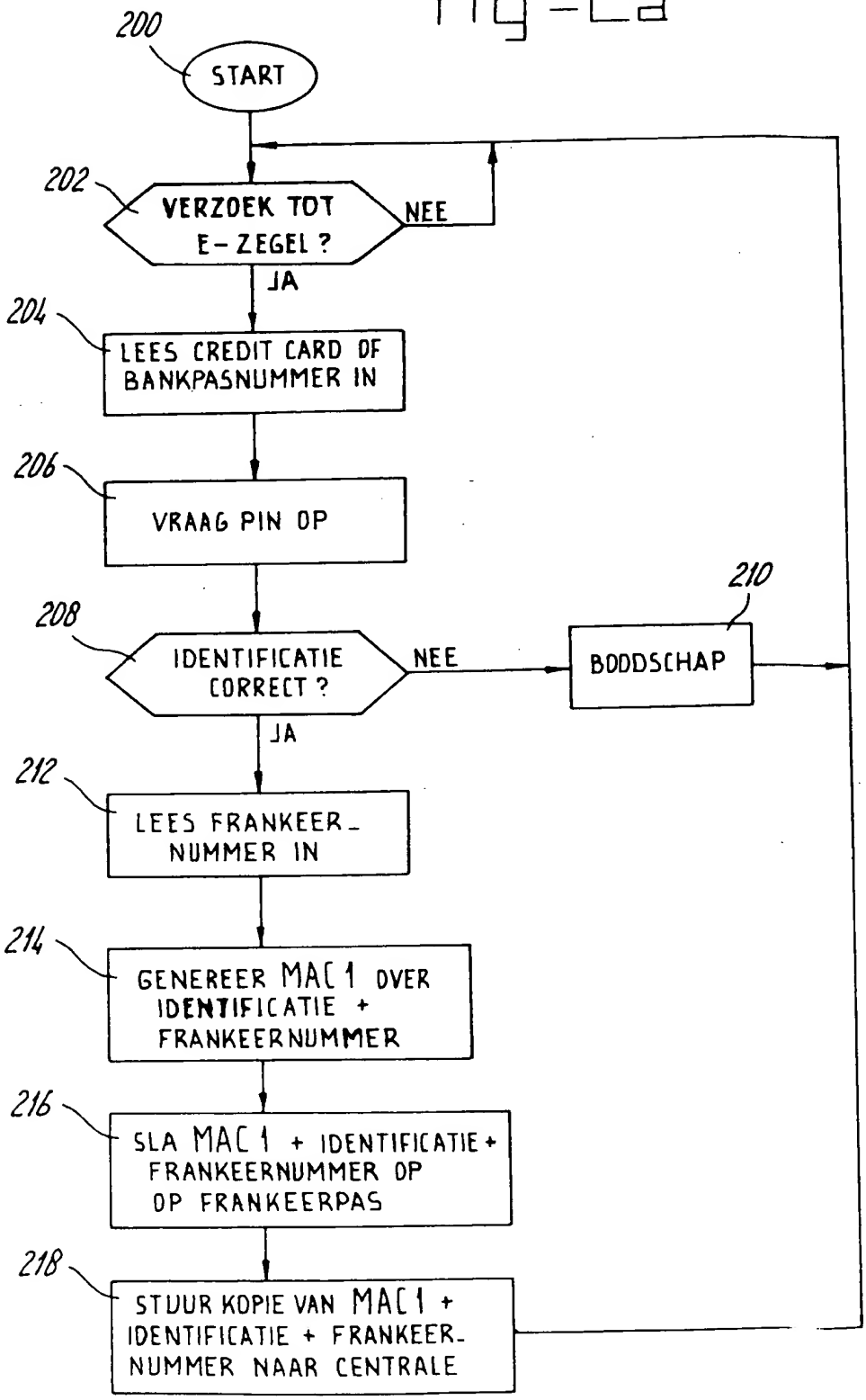

PRO-
CESSOR
PRO-
CESSOR
PSTN
2
3
4
6
8
10
12
14
16
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
34
36
38
40
42
44
46

Fig-1

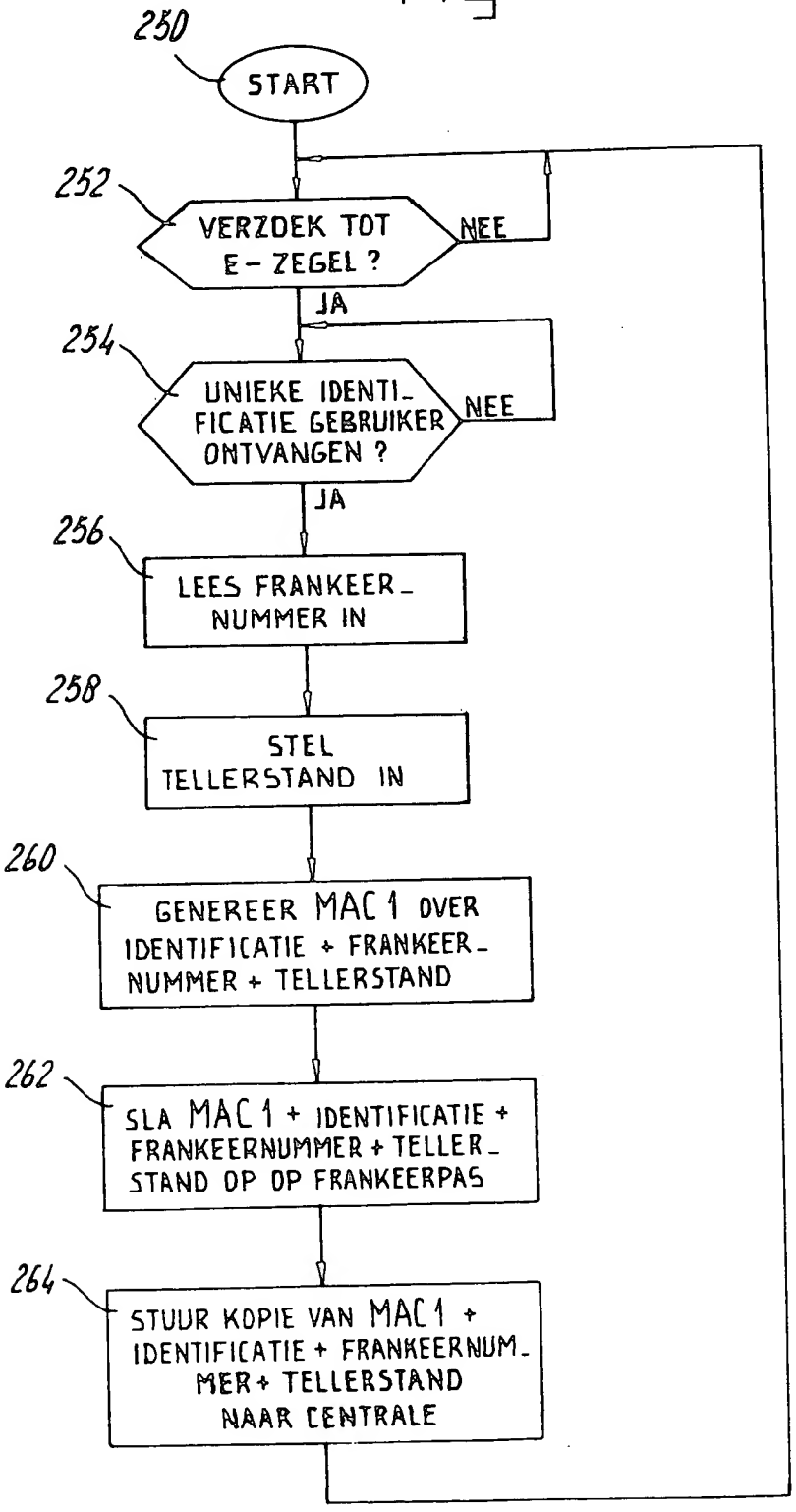
fig-2a



E - ZEGELUITGIFTE

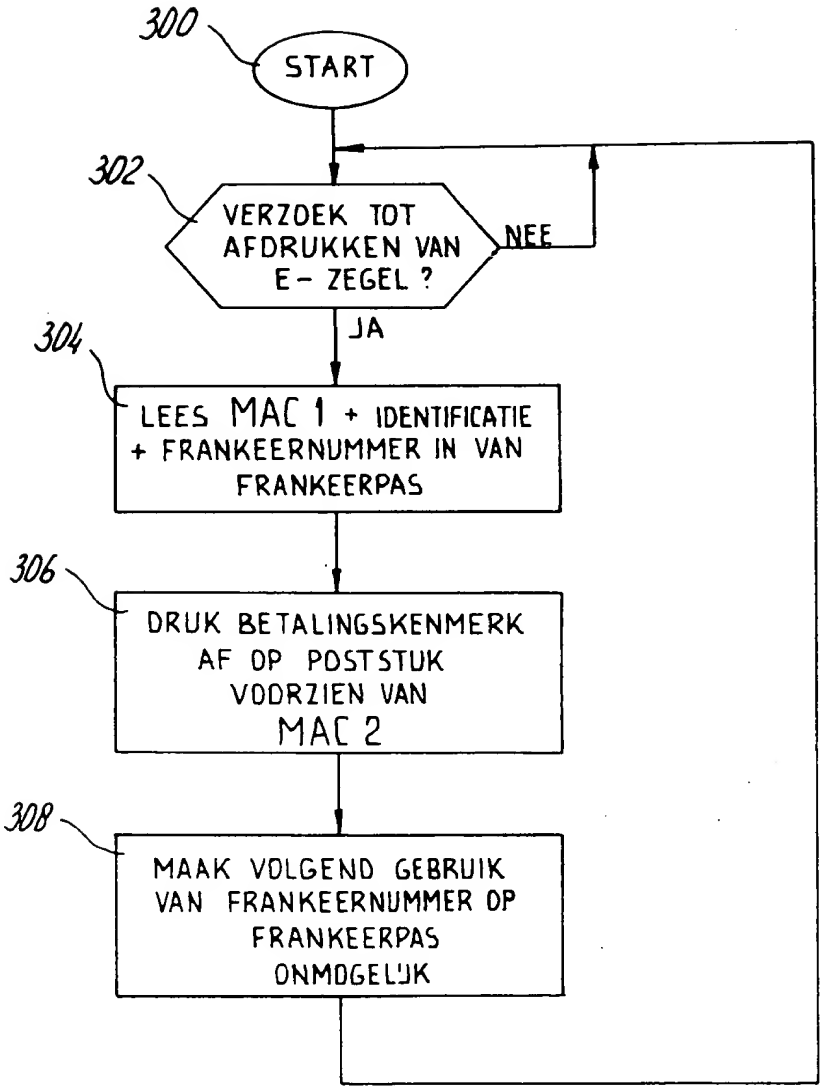
9II B

Fig-2b



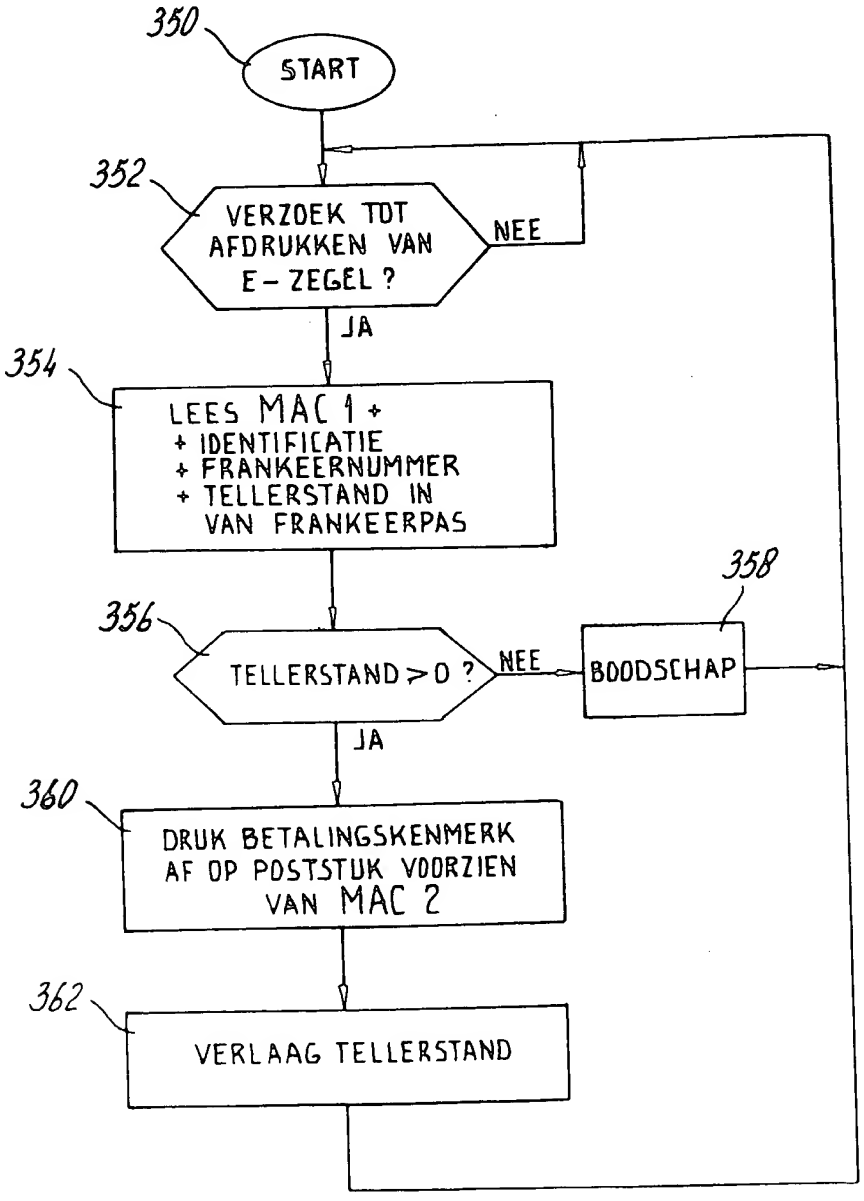
E-ZEGELUITGIFTE MET TELLER

fig - 3a



AFDRUKKEN VAN E- ZEGEL

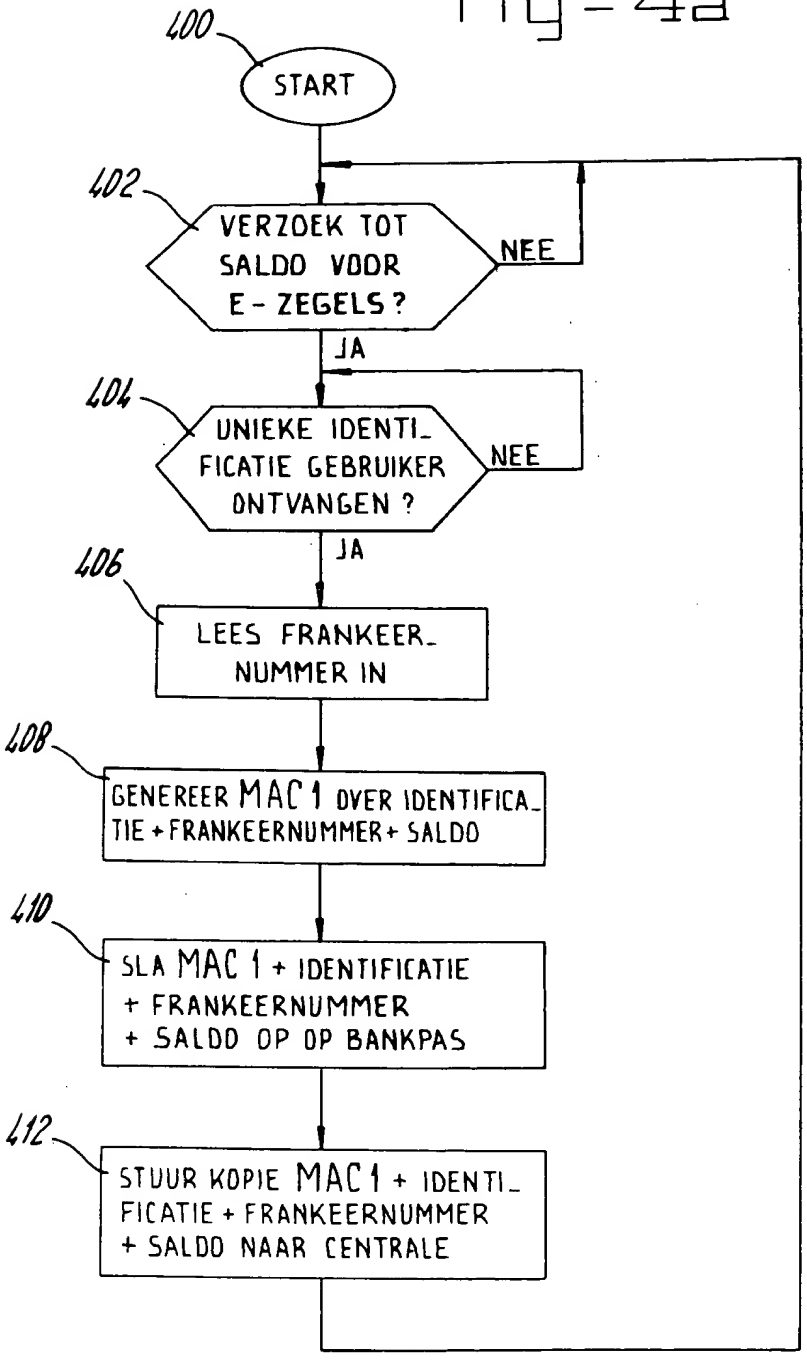
Fig - 3b



AFDRUKKEN MET TELLER

9 II E

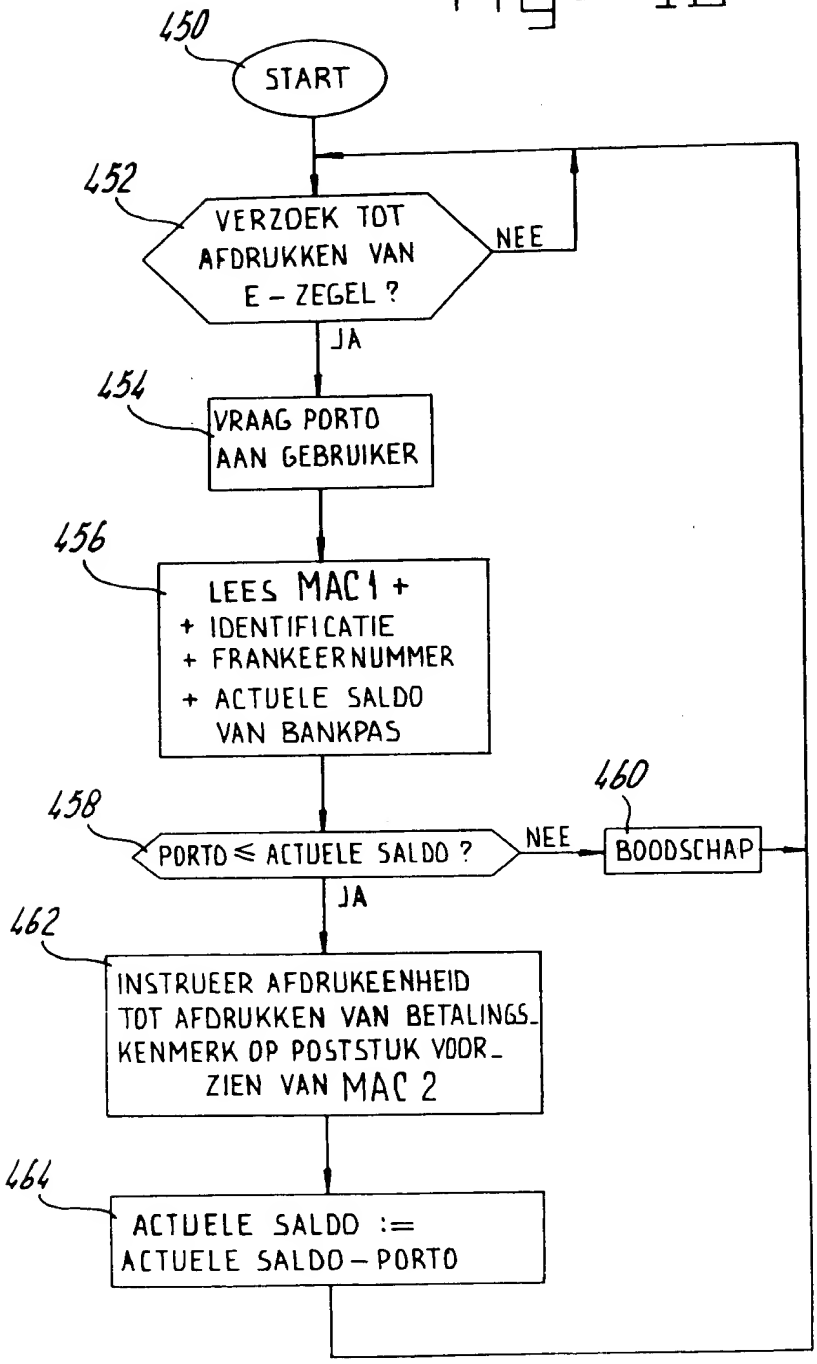
Fig-4a



E-ZEGEL OPSLAG MET PC-UITVOERINGSVORM

9 II F

Fig-4b



AFDRUKKEN VIA
PC-UITVOERINGSVORM

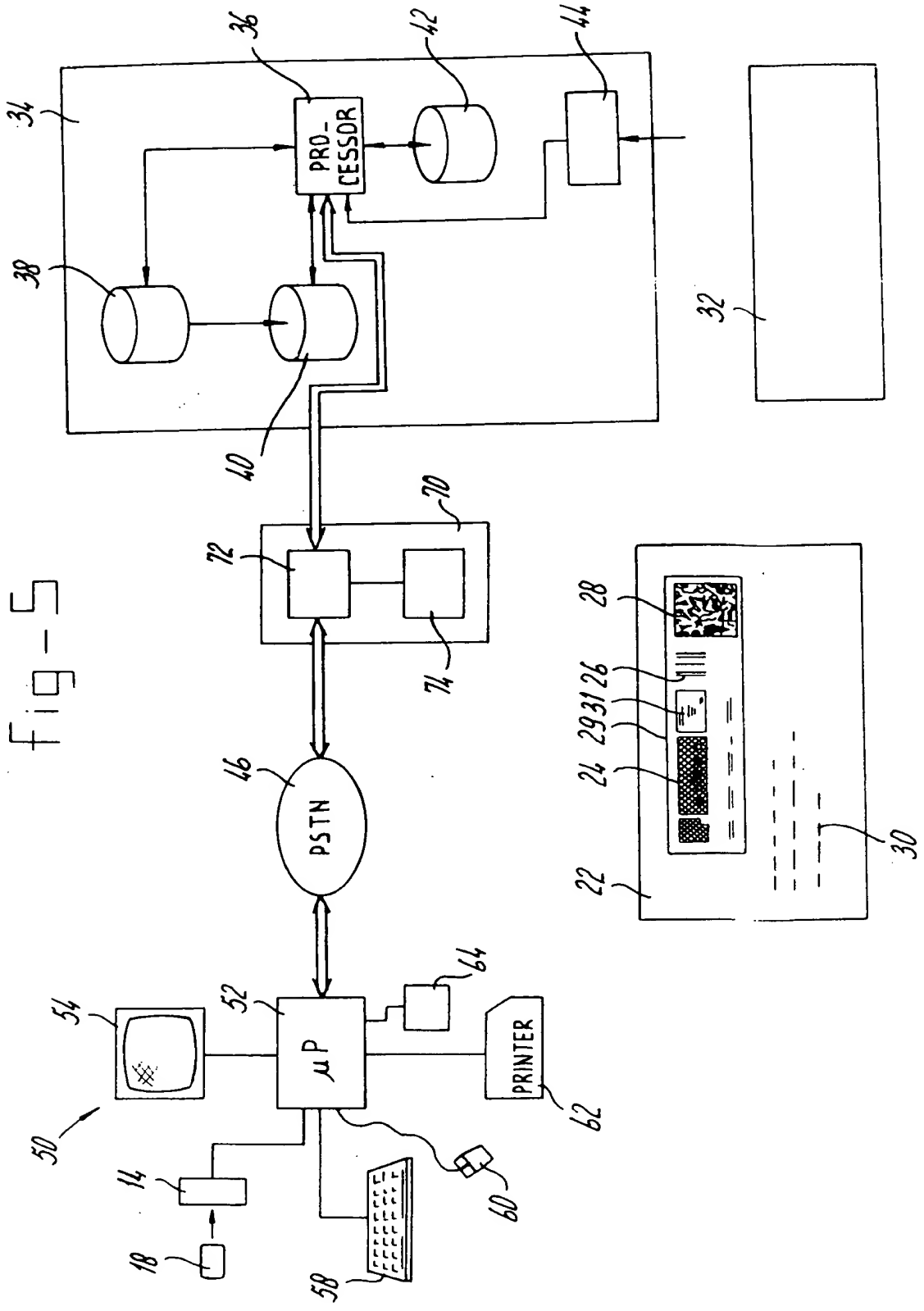

34
36
PRO-
CESSOR
42
44
38
40
32
20
72
74
46
PSTN
28
26
29
31
24
22
30
64
52
µP
54
PRINTER
62
50
14
18
58
60

Fig-5

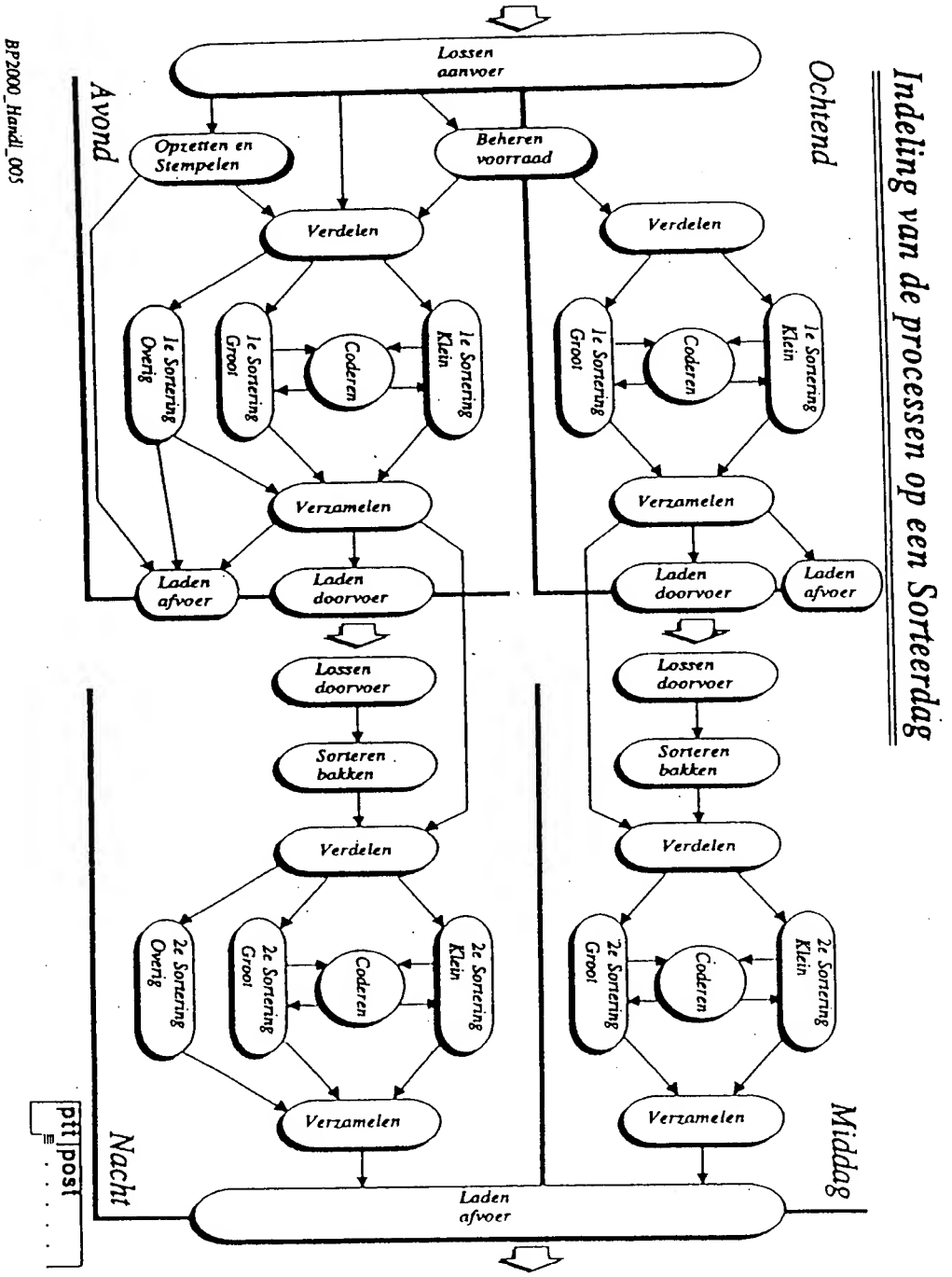

Indeling van de processen op een Sorteerdag
BP2000_Handl_005
Avond
Ochtend
Nacht
Middag
Lossen aanvoer
Opzetten en Stempelen
Beheren voorraad
Verdelen
Verdelen
1e Sortering Overig
1e Sortering Groot
Coderen
1e Sortering Klein
1e Sortering Groot
Coderen
1e Sortering Klein
Verzamelen
Verzamelen
Laden afvoer
Laden doorvoer
Laden doorvoer
Laden afvoer
Lossen doorvoer
Lossen doorvoer
Sorteren bakken
Sorteren bakken
Verdelen
Verdelen
2e Sortering Overig
2e Sortering Groot
Coderen
2e Sortering Klein
2e Sortering Groot
Coderen
2e Sortering Klein
Verzamelen
Verzamelen
Laden afvoer
ptt post

Fig. 6

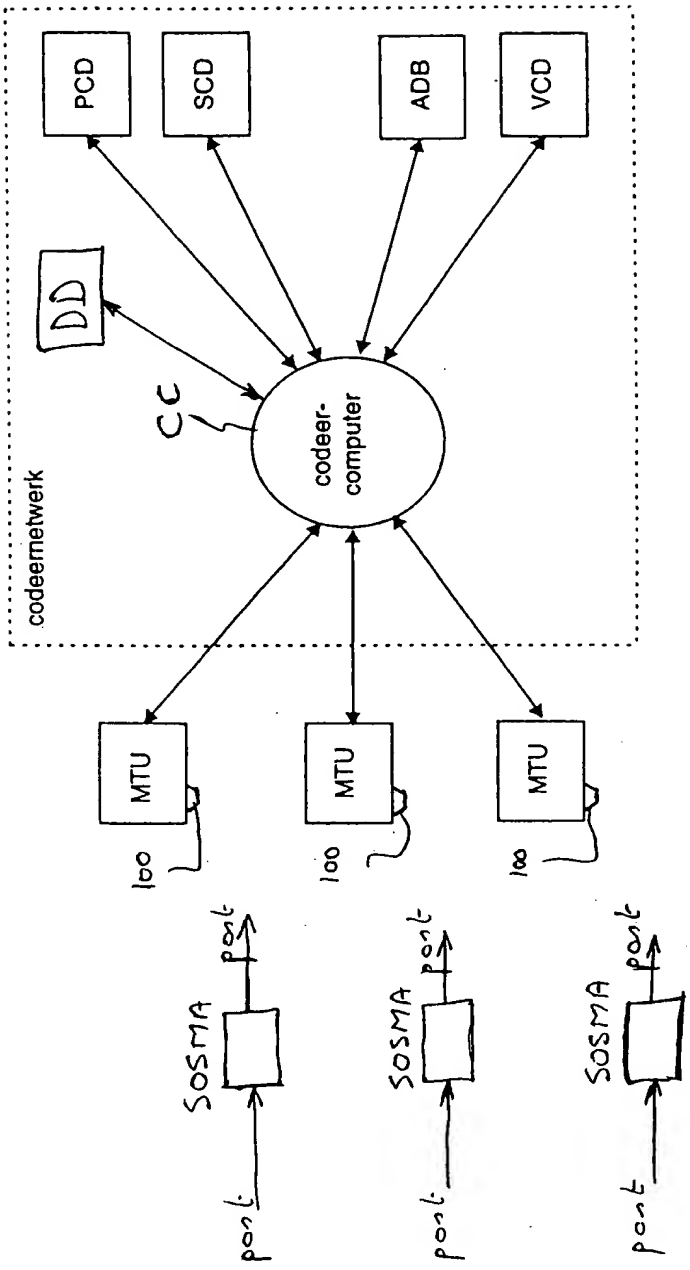

PCD
SCD
ADB
VCD
DD
CC
codeer-computer
codeernetwerk
MTU
MTU
MTU
100
100
100
SOSMA
SOSMA
SOSMA
poort
poort
poort
poort
poort
poort

Fig. 7

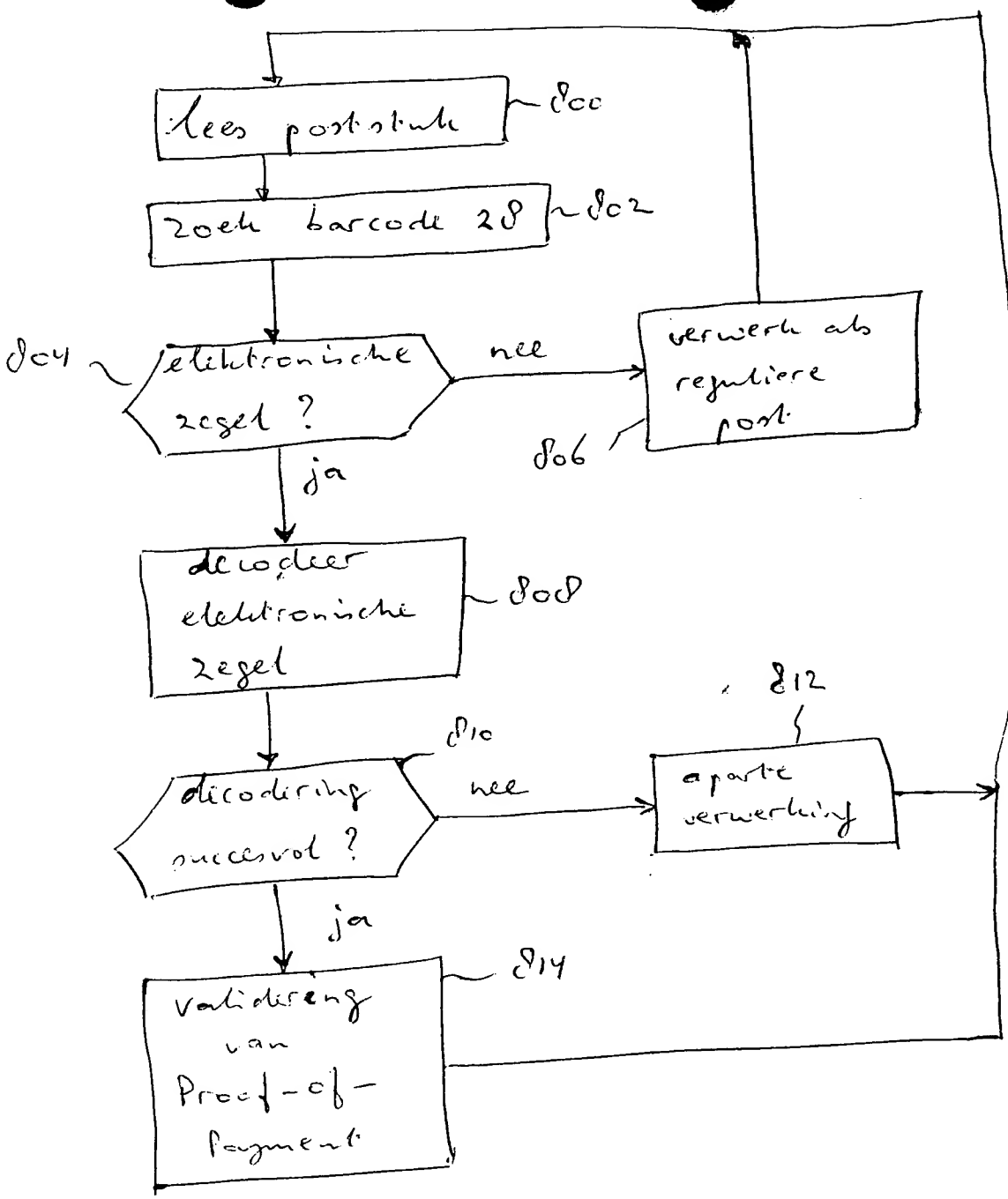

lees poststuk
800
zoek barcode 28
802
elektronische regel ?
804
nee
verwerk als reguliere post
806
ja
decodeer elektronische regel
808
decodering succesvol ?
810
nee
aparte verwerking
812
ja
validering van Proof-of-Payment
814

Fig. 8

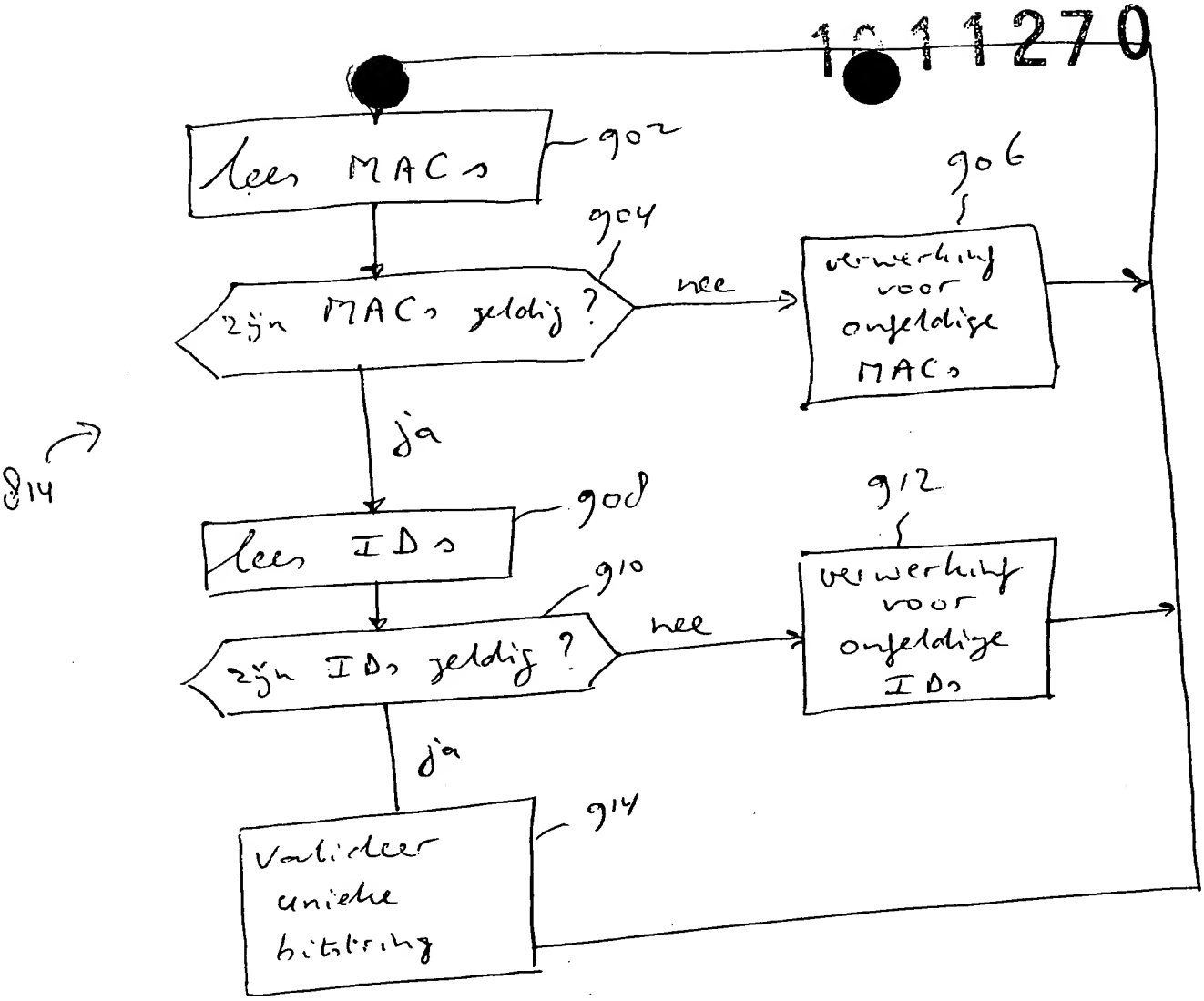

lees MAC's
902
zijn MAC's geldig ?
904
nee
verwerking voor ongeldige MAC's
906
ja
914
lees ID's
908
zijn ID's geldig ?
910
nee
verwerking voor ongeldige ID's
912
ja
valideer unieke bitstring
914

Fig. 9

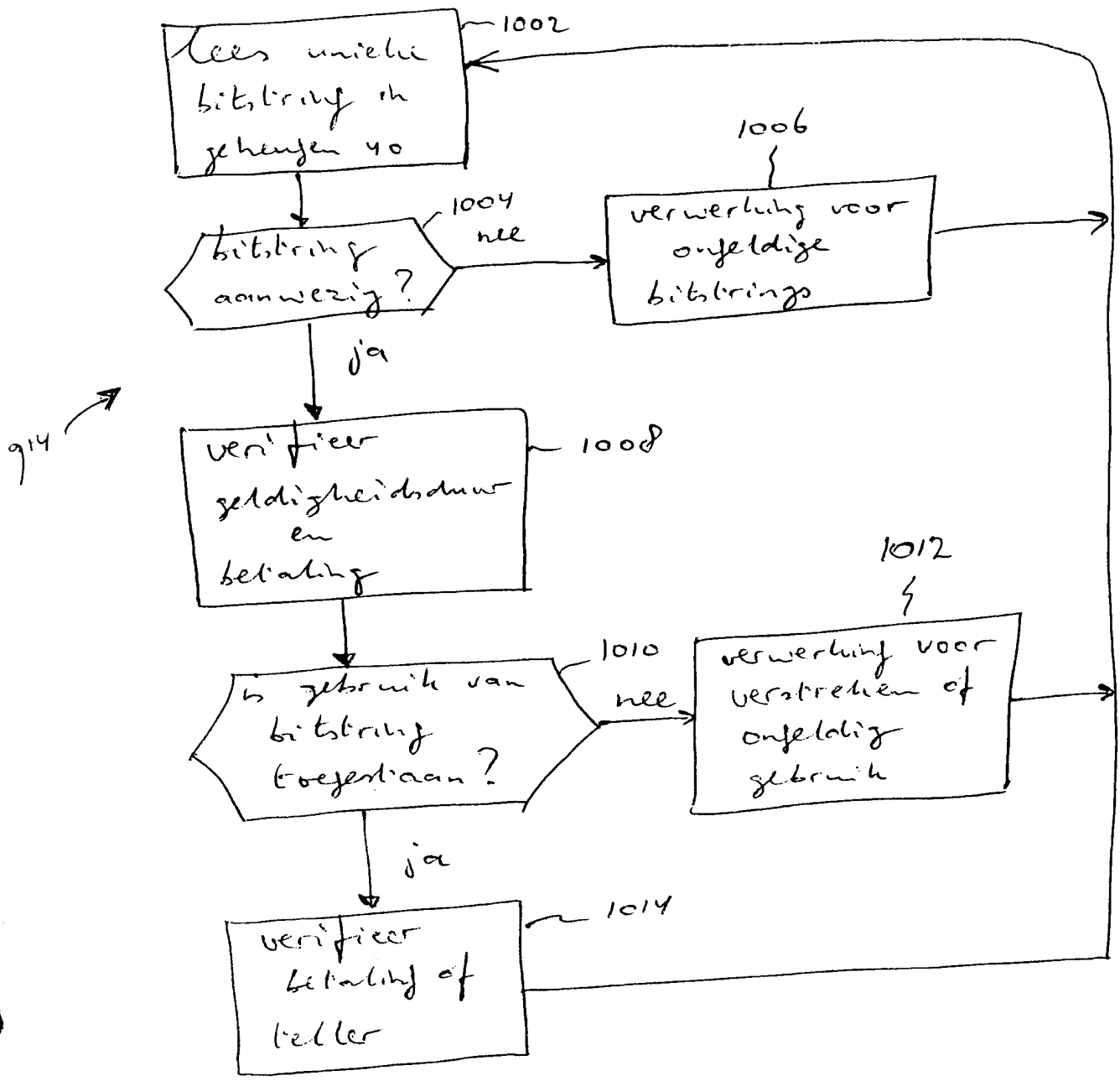

lees unieke bitstring in geheugen 40
1002
bitstring aanwezig?
1004
nee
verwerking voor ongeldige bitstrings
1006
ja
914
verifieer geldigheidsduur en betaling
1008
is gebruik van bitstring toegestaan?
1010
nee
verwerking voor verstrekken of ongeldig gebruik
1012
ja
verifieer betaling of teller
1014

Fig. 10

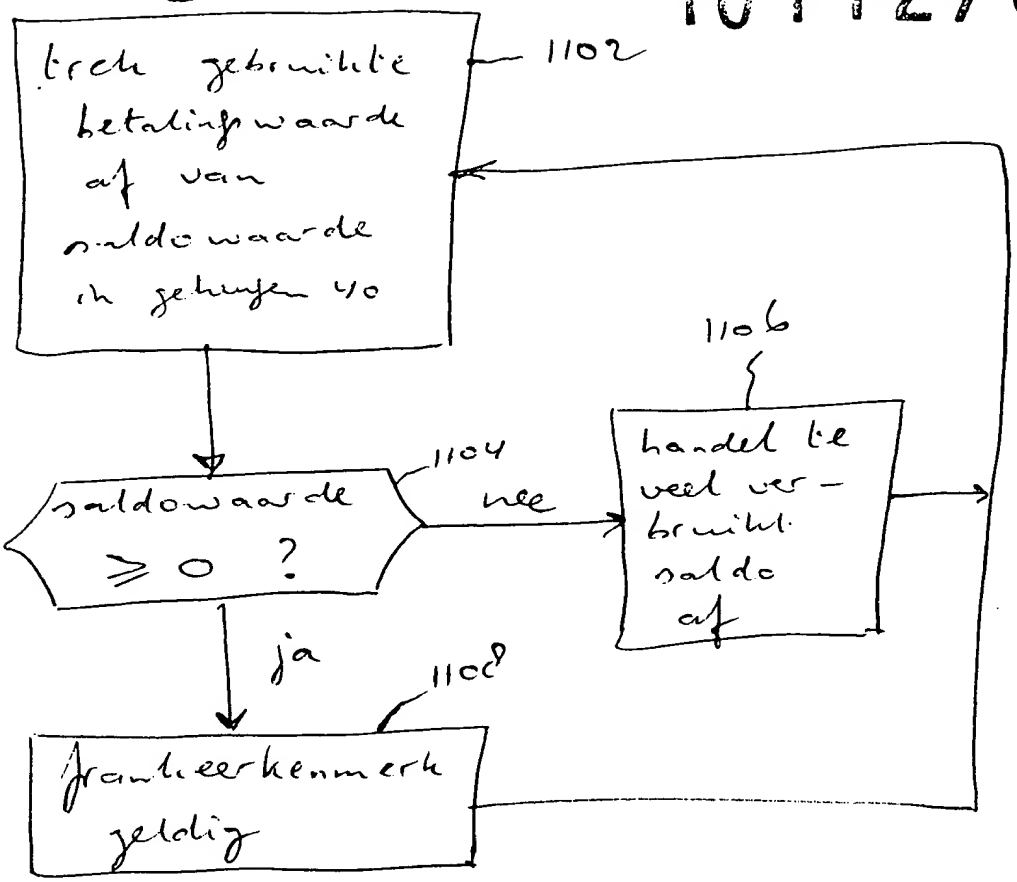

trek gebruikte betalingswaarde af van saldowaarde in geheugen 40
1102
1106
handel te veel verbruikt saldo af
1104
saldowaarde ≥ 0 ?
nee
ja
1108
frankeerkenmerk geldig

Fig. 11

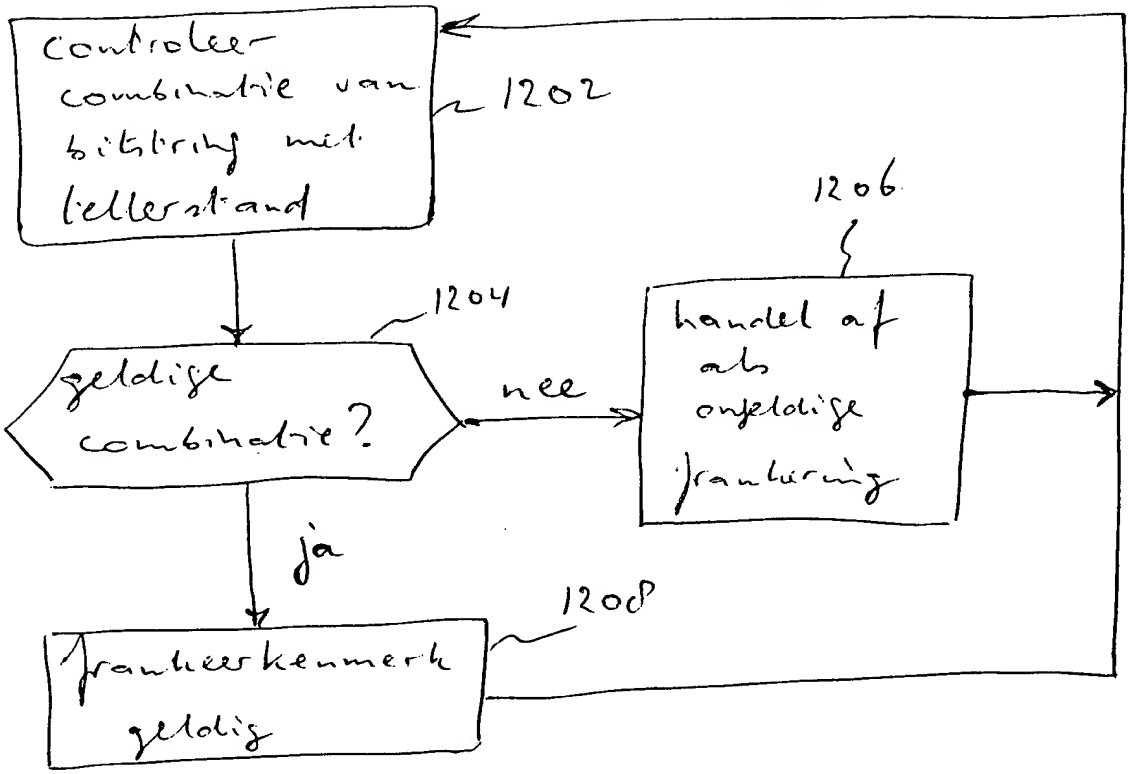

Controleer combinatie van bitstring met tellerstand
1202
1206
1204
geldige combinatie?
nee
handel af als ongeldige frankering
ja
1208
frankeerkenmerk geldig

Fig. 12.

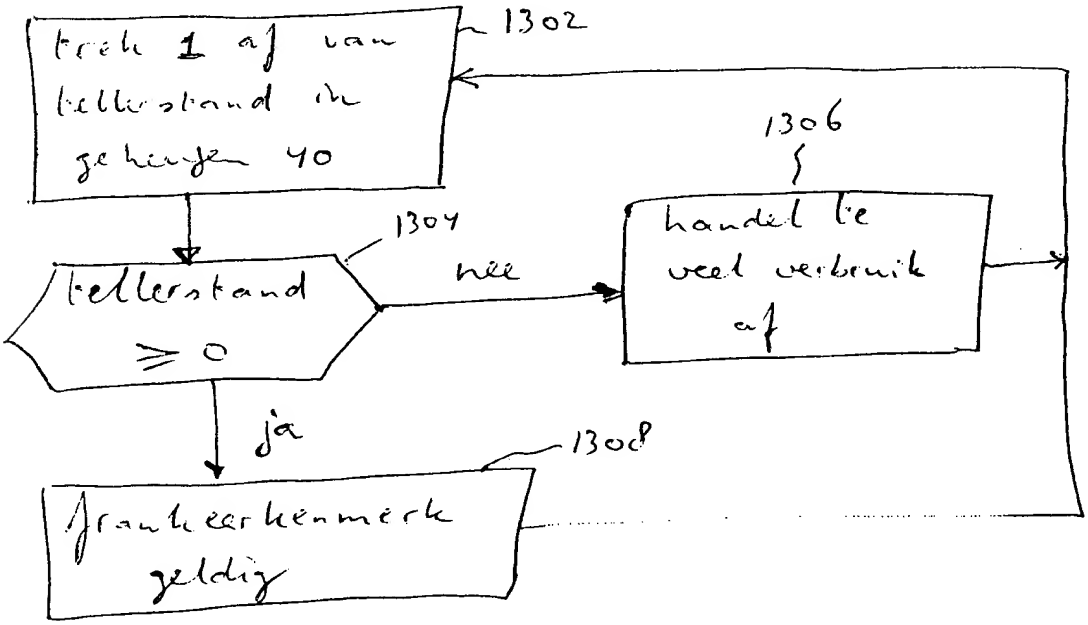

trek 1 af van tellerstand in geheugen 40
1302
1306
1304
tellerstand ≥ 0
nee
handel te veel verbruik af
ja
1308
frankeerkenmerk geldig

Fig. 13

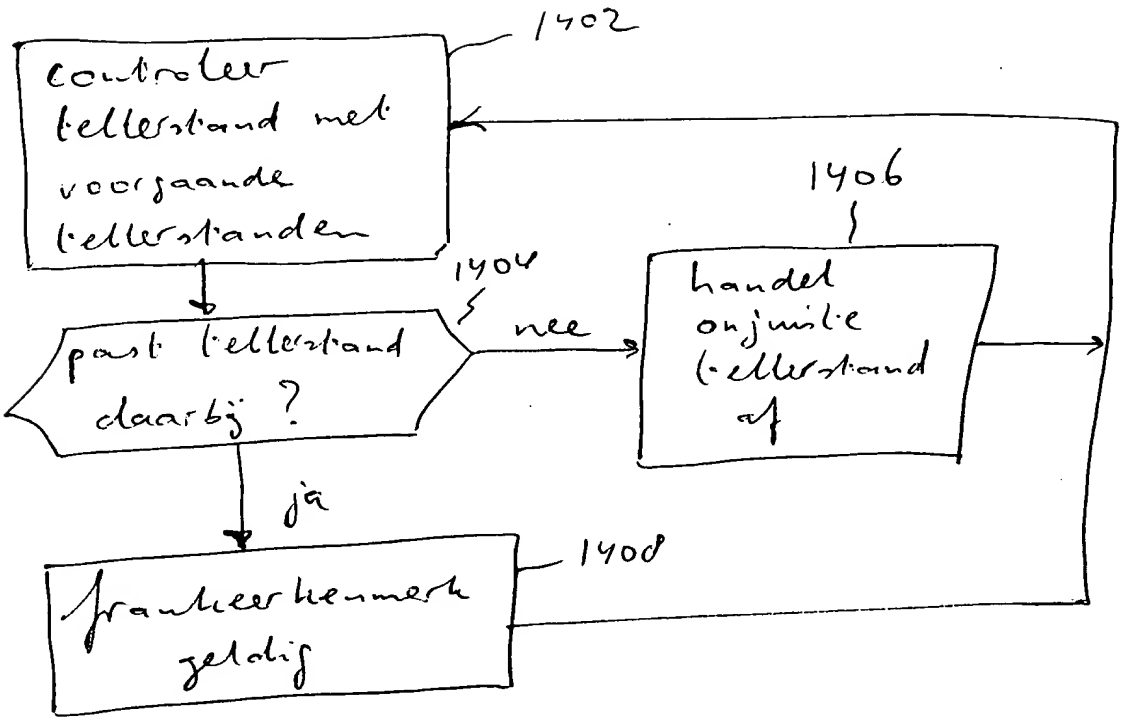

1402
controleer
tellerstand met
voorgaande
tellerstanden
1406
1404
past tellerstand
daarbij ?
nee
handel
onjuiste
tellerstand
af
ja
frankeerkenmerk
geldig
1400

Fig. 14.

gII 0

THIS PAGE BLANK (USPTO)